修士論文

悪性 IP アドレスの分布情報に基づいた
未知の Web サイト判別手法

公立はこだて未来大学大学院　システム情報科学研究科
情報アーキテクチャ領域

金澤　しほり

指導教員　　中村　嘉隆

提出日　2018 年 2 月 19 日

Master's Thesis

Classification method of unknown websites based on distribution information of malicious IP addresses

by

Shihori KANAZAWA

MSc Thesis at Future University Hakodate

Supervisor Prof. Yoshitaka NAKAMURA

Submitted on February 19, 2018

Graduate School of Systems Information Science
Future University Hakodate

Abstract

In recent years, the threat of attacks by viruses and malware on the Internet are increasing year by year. As an example of attack, cyber-attacks through website such as Drive-by download attacks or phishing attacks increase rapidly. The attackers acquire personal information of users illegally by these attacks and causes economic damage. In order to prevent such damage, it is necessary to detect malicious website that cause economic damage. As a countermeasure method, there are several methods for detecting when the website of the access destination is an malicious website and methods for blocking access. The Web reputation system has a function of block malicious website. If the connected domain name is judged to be malicious, the system blocks the access. In this way, the Web reputation system prevents damage caused by malicious programs and phishing s. However, the Web reputation system can block only access to websites clearly made fraudulent activity such as virus distribution and phishing scams. Also, Intrusion Detection System (IDS) is a system that detects illegal packets flowing on the network. IDS constantly monitors packets flowing in the network and checks for unauthorized intrusion or attack. In addition, IPS supports sophisticated and advanced security threats such as bot attacks and DoS attacks that are considered to be difficult to protect only by general firewalls and anti-virus software. Intrusion Prevention System (IPS) examines the contents and behaviors of communication packets, and blocks web access if IPS detects communication as malicious. However IDS and IPS can only detect known suspicious packets included in the Web access communication. Since the above two methods use known information such as information of suspicious packets included in known malicious website, there is an advantage that the detection rate of known malicious website is relatively high. However, these methods have drawbacks that cannot be detected unknown malicious website. Therefore, we propose a method to detect and classify an unknown malicious website.

The detection based on blacklists is mainstream in the detection method of conventional malicious website. There are the detection methods using domain name features for unknown malicious website not on blacklists. However, since it is relatively easy to change the domain name, it is inappropriate for the method of detecting malicious websites by using domain names. On the other hand, it is difficult to change the IP address once it is set. Therefore, in this research, we focus on IP addresses that are difficult to change, and propose the detection methods corresponding to unknown website. Also, we analyzed the features of IP addresses used for malicious activities to distinguish unknown malicious website. As a result, malicious IP addresses were found to show differences in usage frequency of each IP address class. Also, the features of malicious IP addresses change over time. Therefore, we proposed the method using features of the network address part of the IP address class to classify unknown website.

In this paper, since the time changes in the usage features of malicious IP address are recognized, we conducted evaluation experiments to confirm the influence on the classification performance and to determine the composition of the optimal classifiers. From the experimental results by classifiers using blacklist itself, since the accuracy was achieved low values, the classification of malicious website using blacklist has low generalization ability and has no ability to deal with unknown website. From the experimental results by classifiers using the features of IP addresses on blacklist without assuming time change, high classification accuracy was achieved in IP address Class A, and we confirm the effectiveness of the proposed classification method. On the other hand, as for the addresses of IP address class B and IP address class C, overall accuracy is lower than those of IP address class A. Also, it is possible to improve classification accuracy by considering time changes of features of malicious IP addresses.

Keywords: cyber-attack, malicious website, network address, IP address of Class

概要

近年, Drive-by download 攻撃やフィッシングなど Web サイトを介したサイバー攻撃が急増しており，ユーザの個人情報等が不正に取得され，経済的被害を受ける事件が増加している．そのため，経済的な被害をもたらす悪質な Web サイトを検出することが重要である．対策方法として，アクセス先の Web サイトが不正 Web サイトである場合に検知する方法や，アクセスを遮断する方法がいくつか存在する．Web レピュテーションシステムは，不正 Web サイトブロック機能を持つソフトウェアで実現されている. ユーザによる Web アクセス通信が発生する際に，接続先のドメイン名や Web サイトが不正であると判断された場合には，そのアクセス自体をブロックすることによって，不正プログラムによる感染，およびフィッシングによる被害を防止している．しかし，このとき不正 Web サイトとして判断されるものは，すでにウイルス配信, フィッシング詐欺など, 不正行為を行ったことが確認された Web サイトに限られる. また，IDS（不正侵入検知システム）は，ネットワーク上を流れる不正なパケットを検知するシステムであり，ネットワークに流れるパケットを常時監視し，不正侵入や攻撃がないかチェックするものである．さらに，IPS（不正侵入検知システム）は，ファイアウォールやアンチウイルスソフトウェアのみでは防御が困難とされていた DoS 攻撃やボットによる攻撃など, 巧妙かつ高度なセキュリティの脅威にも対応しており，Web サイトへアクセス通信が行なわれた際に，通信に含まれる不審な通信パケットを検出して，その通信を遮断する仕組みになっている．しかし，IDS や IPS による検出も，Web アクセス通信に含まれる既知の不審パケットのみに限られる．前述した 2 つの方法は，既知の不正 Web サイトに関しては検出率が高いが，未知の不正 Web サイトに対応した検出が困難である．そこで，本研究では，経済的被害の原因となる未知の不正 Web サイトを検出して，正規と不正に判別することを目的とする．

従来の不正 Web サイトの検出手法では，ブラックリストに基づいた検出が主流であり，ブラックリストに存在しない未知の不正 Web サイトに対してはドメイン名の特徴を用いた検出手法が多く見られる．しかし，ドメイン名は変更が容易であるため，攻撃者は検出回避のために頻繁にドメイン変更を行っている問題がある．一方，IP アドレスは，一旦設定されると更新することは困難であるという特徴がある．そこで，容易に変更されづらい IP アドレスに着目し，未知の Web サイトに対応した検出手法を提案する．また，未知の不正 Web サイトの判別を行うために，悪質な活動に利用される IP アドレスの分布特徴について分析した．その結果，IP アドレスクラスごとに悪性 IP アドレスの利用頻度に差があることが判明した．また，悪性 IP アドレスの分布特徴には経年変化が見られることが判明した．そこで，IP アドレスクラスのネットワークアドレス部を特徴として未知の不正 Web サイトの判別に用いる．

本論文では，悪性 IP アドレスの利用分布の経年変化が判別性能に与える影響を把握し，最適な判別器の構成を決定し，提案手法の有効性を検証するために評価実験を行った．ブラックリストのみを用いた不正 Web サイトの検出は，低い精度を示したことから，汎化能力が低く，未知の Web サイトに対応できる能力を持たないといえる. ブラックリストの変化による分類器の再学習なしの判別手法については，IP アドレスクラス A において高精度な判別ができ，有効性を確認できた．一方で，IP アドレスクラス B および IP アドレスクラス C における判別精度はそれほど高い結果が得られなかった．これに対して，ブラックリストの変化による分類器の再学習ありの判別手法を用いた場合, 悪性 IP アドレスの特徴の経年変化を考慮した判別を行うことにより，判別精度の向上が見られた．

キーワード: サイバー攻撃，不正 Web サイト，ネットワークアドレス，IP アドレスクラス

目次

第1章　序論

1.1　背景

近年，インターネット上で，ウイルスやマルウェアによる攻撃の脅威が年々増加している[1][2]．その中で，特に Web サイトを利用した攻撃が急増している[3][4]．2017 年 3 月に IPA(独立行政法人情報処理推進機構)が発表した「2017 年版 情報セキュリティ 10 大脅威」[4]の中で，個人に向けられた脅威のランキングによると，1 位（インターネットバンキングやクレジットカード情報の不正利用）と 4~6 位（ウェブサービスへの不正ログイン，ワンクリック請求などの不当請求，ウェブサービスからの個人情報摂取）の 4 つが Web サイトに対する攻撃となっている．また，組織に向けられた脅威ランキングでは，3 位（ウェブサービスからの個人情報摂取），6 位（ウェブサイトの改ざん），7 位（ウェブサービスへの不正ログイン），10 位（インターネットバンキングやクレジットカード情報の不正利用）の 4 つが Web サイトに対する攻撃となっている[4]．これらの被害を引き起こす攻撃パターンとして，ユーザが Web サイトを閲覧した際に，ウイルスやマルウェアなどの不正プログラムをパソコンにダウンロードさせる Drive-by download 攻撃や，金融機関を装った偽のサイトへ誘導するフィッシング詐欺，利用者が攻撃者が用意した悪意のあるウェブサイトにアクセスしたり，メールに添付されている悪意のあるファイルを開いたりすることで，ウイルスに感染させるウイルス感染が挙げられる．また，これらの攻撃により，閲覧者のパソコンでマルウェアが活動し，保管されたデータやプログラムを破壊される事件や，暗証番号やクレジットカード番号などの個人情報を不正に取得され，経済的な被害を受ける事件が増加している．図 1 は，2011 年から 2015 年までの警察庁広報資料「インターネットバンキングに係る不正送金事犯発生状況」の発生件数と被害額データを示している[1][2].

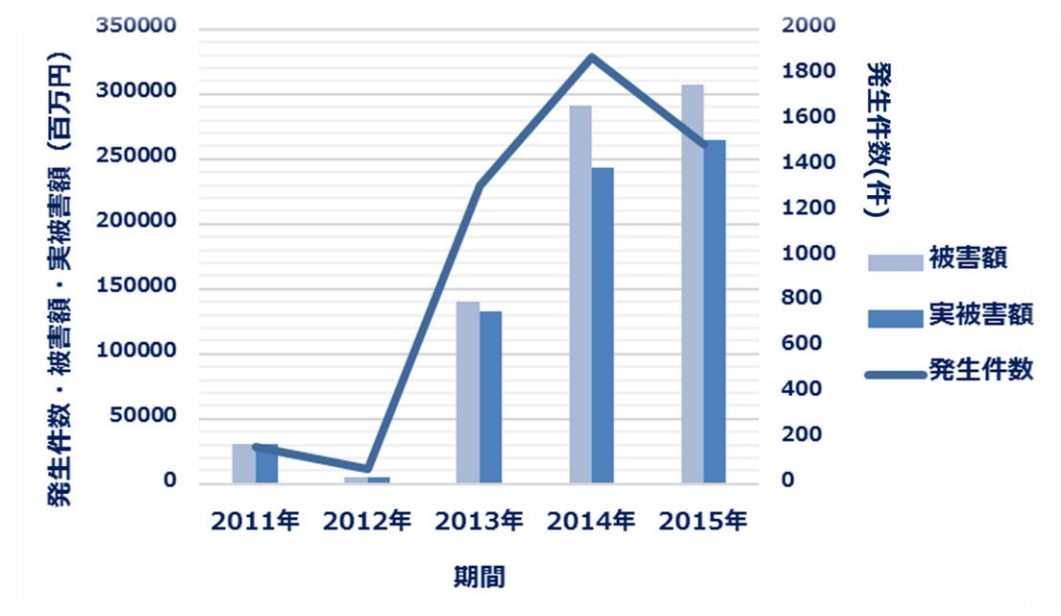


図 1　インターネットバンキングに係る不正送金事犯発生状況(文献[1][2]から引用)

Figure 1　The number of incidents, damage amount, and actual amount

文献[1][2]によると，インターネットバンキングを介して，個人情報が不正に取得され，経済的被害を被った件数は，2012 年まで 50 件程度であったのに対し，2015 年には 1400 件近くまで急増しており，現在も増加傾向にある．被害件数が徐々に減少しているが，個人口座の被害額は引き続き大きいため，警戒が必要である．このような被害を防ぐため，ユーザが不正 Web サイトにアクセスしないように対策を行う必要がある．対策方法として，アクセス先の Web サイトが不正 Web サイトである場合にシステムで検知する方法や，アクセスを遮断する方法がいくつか存在する．その方法の一つとして，Web レピュテーションシステム[5][6][7]が開発されている．Web レピュテーションシステムは，不正 Web サイトブロック機能を持つソフトウェアで実現されている．ユーザによる Web アクセス通信が発生する際に，接続先のドメイン名や Web サイトが不正であると判断された場合には，そのアクセス自体をブロックすることによって，不正プログラムによる感染，およびフィッシングによる被害を防止している．しかし，このとき不正 Web サイトとして判断されるものは，すでにウイルス配信，フィッシング詐欺など，不正行為を行ったことが確認された Web サイトに限られる．また，Intrusion Detection System (IDS, 侵入検知システム)[8]や， Intrusion Prevention System（IPS，侵入防止システム）[8][9]を用いる方法もある．

IDS は，ネットワーク上を流れる不正なパケットを検知するシステムである．IDS は，大きく分けて，ネットワーク型とホスト型に分けられる．ネットワーク型 IDS は，監視対象となるネットワークに別機器として設置する．ネットワークに流れるパケットを常時監視し，不正侵入や攻撃がないかチェックするものである．一方，ホスト型 IDS は，監視対象となるシステムに直接インストールする形で設置する．システムに侵入しようとする攻撃を検知する機能や，システム内のファイルの改ざんなどをチェックすることも可能である．しかし，IDS は，あくまで「検知」に主眼を置いたシステムであり，実際には検知したことを管理者に連絡・通知するものの，何らかの防御手段をとるわけではない．したがって，不正侵入・データ改ざんが発生した場合，侵入・改ざん検知の通知を受けた管理者が対応するという手順が必要となり，対応にタイムロスが発生してしまう．そこで，IDS に防御機能を持たせたシステムとして，IPS が開発されている．

IPS は，ファイアウォールやアンチウイルスソフトウェアのみでは防御が困難とされていた DoS 攻撃やボットによる攻撃など，巧妙かつ高度なセキュリティの脅威にも対応している．Web サイトへアクセス通信が行なわれた際に，通信に含まれる不審な通信パケットを検出して，その通信を遮断する仕組みになっている．IDS や IPS で不正アクセスなどの攻撃を検出する方法は，大きく分けて，不正検出型と異常検出型に分けられる．不正検出型は，あらかじめシグネチャと呼ばれる攻撃パターンを集めたデータベースを持っており，攻撃がそのパターンに一致した場合，不正なものとみなして通信を遮断する．一方，異常検出型は，問題がない正常な動作をホワイトリストとして持たせておき，そのパターンから外れるものを不正な攻撃と判断して遮断する．

前述した 2 つの方法は，既知の不正 Web サイトや，不正 Web サイトに対するアクセス通信に含まれる既知の不審パケットなど，既知の情報を用いているため，既知の不正 Web サイトに関しては検出率が高いという利点がある．しかし，未知の不正 Web サイトに対応した検出が困難であり，仮に検出できた場合であっても，十分な精度が得られるか不明である．このような問題点を解決するために，不正 Web サイトの様々な特徴を用いて，未知の不正 Web サイトの検出率を向上する研究[10][11][13][14][15][16]が盛んに行われている．しかし，用いる不正 Web サイトの特徴によっては，検出からの回避が容易であったり，特徴を最新に維持することが困難な状態であることが多い．また，検出するためのコストや負荷が大きいことも問題点として挙げられる．したがって，未知の不正 Web サイトの検出にあたり，容易に検出を回避されにくく，検出にかかるコストを軽減することができる不正 Web サイトの特徴を検出条件として設定

することが検出に有効であると考える．また，検出された未知の Web サイトが，不正 Web サイトか正規 Web サイトか分類する必要がある．

以上より，本論文では，未知の不正 Web サイトに対応した検出と判別手法を提案する．アプローチとしては，検出された Web サイトを既知の Web サイトか未知の Web サイトのどちらかに分類した上で，未知の Web サイトに対して正規 Web サイトか不正 Web サイトを判別する．

1.2 研究目標

本研究では，低コストで未知の不正 Web サイトを高精度に判別する手法を提案することを研究目的とする．未知の不正 Web サイトを検出，及び判別するにあたり，用いる不正 Web サイトの特徴を厳選する必要がある．そのため，検出から回避されにくく，検出や判別の負荷が小さくすることが可能である特徴を考慮する必要がある．また，既存手法で用いられている不正 Web サイトの特徴は，特定の環境を整えた上で使用する必要があるなど，環境依存である可能性もある．そのため，環境依存が少なく，汎用性の高い特徴を選択する必要がある．したがって，不正 Web サイトの特徴を分析し，その分析に基づく未知の不正 Web サイトの判別手法を検討する．それとともに，既存手法よりも，低コストで，未知の不正 Web サイトの判別精度の向上を図り，汎用性の高い未知の不正 Web サイト判別手法を提案する．

1.3 システム情報科学における本研究の位置付け

本研究は，未知の不正 Web サイトの判別精度の向上を図る研究として位置付けられる．近年，悪質な活動が行われた通信や，ブラックリストから得られるデータを蓄積し分析する研究が盛んに行われている．また，蓄積したデータを他分野へ利用することにより，収集したデータに新たな価値を見出すことが期待される．

本研究では，低コストで，汎用性の高い未知の不正 Web サイト判別手法の提案を目的としている．一般的に，利用されるブラックリストやホワイトリストを最新に維持することは難しい．また，既存手法は，特定の環境を整えた上で使用されるため，環境依存も生じる．そこで，不正 Web サイトの特徴を分析し，不正 Web サイトの検出，及び判別に有効的な特徴を用いて不正 Web サイトの検知システムからユーザに警告を促すことで，既存のシステムにはない未知の不正 Web サイトの検出，及び判別に活用できると考えている．

1.4 論文の構成

本論文は全 5 章から構成されている．第 1 章は本研究の背景と研究目標およびシステム情報科学における位置づけについて述べる．第 2 章では研究目的である未知の不正 Web サイト判別を行うにあたって，既存の未知の不正 Web サイトの検出に関する研究や未知の不正 Web サイトの判別に関する研究について述べる．第 3 章では，未知の不正 Web サイトの判別を実現するためのアプローチについて述べ，その後に本研究の提案手法について述べる．第 4 章では提案手法の評価実験について述べ，実験結果について考察する．最後に第 5 章でまとめと今後の展望について述べる．

第2章　関連研究

本章では，関連研究についてまとめる．まず，未知の不正 Web サイトの検出に関する研究として，ドメイン名の特徴に基づいた検出手法について述べる．次に，未知の不正 Web サイトの判別に関する研究として，IP アドレスの特徴に基づいた判別手法について述べる．最後に，関連研究のまとめと本研究の位置付けについて述べる．本稿では，「検出」を「未知の Web サイトを発見すること」，「判別」を「未知の Web サイトを正規 Web サイトか不正 Web サイトに分類すること」と定義する．

2.1　未知の不正 Web サイトの検出に関する研究

本節では，ドメイン名を用いた不正 Web サイトの検出に関する研究[10][11][13][16]，ドメインリストを用いた不正 Web サイトの検出に関する研究[14]について述べる．

ドメイン名の特徴に基づいた検出手法には，劉ら[11]の，不正 Web サイトに見られるドメイン名の特徴を検出条件として用いる手法や，L. Bilge ら[13]の，DNS 分析技術を用いて悪質な活動に関与するドメイン名を検出する手法，田中ら[14]の，マルウェアが通信を行う際の特徴を利用して，DNS 通信の観測によって未知の不正 Web サイトを検出する手法などがある．

文献[10]は，不正 Web サイトに見られるドメイン名の特徴を検出条件として用いている．不正 Web サイトのドメイン名は，英数字がランダムに混在するものが多い傾向にあるため，英数字が混在するドメイン名を利用しているかどうかを 1 つ目の検出条件としている．また，不正 Web サイトのドメイン名は，ボットに感染したコンピュータ群(ボットネット)を利用してフィッシングやウイルス配布などを行う Fast-Flux[12]などの攻撃手法を用いて自動生成されることが多いため，人間にとって扱いにくい 10 文字以上の長い文字列で構成されているものが多い．図 2 は，良性と悪性サイトの FQDN 文字列の長さを比較し，その累積補分布を示す．

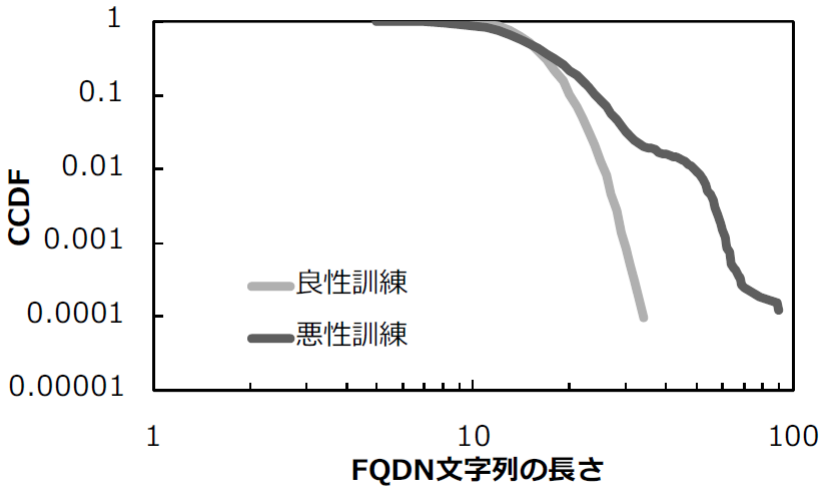


図 2　FQDN 文字列の長さの累積補分布(文献[16]から引用)

Figure 2　Cumulative complementary distribution of length of FQDN character string

FQDN は，DNS（Domain Name System）などのホスト名，ドメイン名（サブドメイン名）などすべてを省略せずに指定した記述形式のことである．図 2 より，悪性 FQDN はより長い文字列で構成されることがわかる．そのため，10 文字以上で構成されるドメイン名であることを 2 つ目の検出条件としている．

文献[13]では，正常なドメイン名と悪性ドメイン名を区別するために複数の特徴を用いている．名前解決動作周期性や様々な悪性ドメインとの IP アドレスの共有，TTL 値の特異性，ドメイン名に乱数が含まれる，といった項目が悪性ドメイン名の特徴として挙げられる．これらの特徴を利用して数カ月にわたる DNS 通信ログの分析を行い, 高い精度で悪性ドメインが検出できることを示している．さらに，この手法を取り入れた解析システムを ISP に導入し，リアルタイムで解析を行った場合にも未知の悪性ドメイン名を検出できることを示している．また，文献[14]は，マルウェアが通信を行う際の特徴を利用して，DNS 通信の観測によって未知の不正 Web サイトの検出を行っている. マルウェアに感染しているクライアントは複数の不正 Web サイトにアクセスを行う傾向にあるため, 不正 Web サイトにアクセスを行ったクライアントは, 他の不正 Web サイトにもアクセスを行っている可能性が高い．そのため，DNS 通信において既知の悪性ドメイン名にアクセスを行っていたクライアントから名前解決要求のあるドメイン名は，マルウェアとの関連が深いドメイン名であるとみなして，未知の不正 Web サイトとして検出する．

これらの手法は, すでに悪性であることが既知であるドメイン名のリスト(ブラックリスト)を使用するため，既知の Web サイトの検出に有効である．しかし，条件に該当しない不正 Web サイトの検出が困難である問題がある．また，ドメイン名は容易に生成・更新することができるため，頻繁に変更されやすく，ブラックリストを常に最新の状態に維持することが困難である．

2.2　未知の不正 Web サイトの判別に関する研究

本節では, IP アドレスを用いた不正 Web サイトの判別に関する研究[15][16]について述べる．

文献[15][16]では，不正 Web サイトを見つけるための判別条件として，不正 Web サイトに見られる IP アドレスの特徴を用いている．不正 Web サイトは，図 3 に示すように特定の IP アドレス群を使用する傾向がある[15][16].

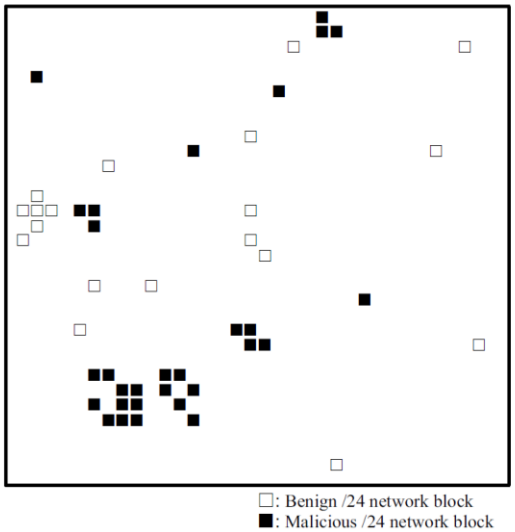


図 3　IP アドレス分布の可視化(文献[15]から引用)

Figure 3　Visualization of IP address distribution (Source: Ref.[15])

文献[15]は，正規 Web サイトと不正 Web サイトそれぞれの IP アドレスをヒルベルト曲線に基づく 2 次元グラフ上に配置している．ヒルベルト曲線とは，再帰的に定義される空間充填曲線のうちの一つであり，この曲線を用いることで，IP アドレスの近接性を維持したまま IPv4 アドレス空間を 2 次元グラフとして視覚化できる．図 3 は，あるネットワークアドレスブロック x.0.0.0/24 の IP アドレスの配置をヒルベルト曲線によって視覚化したものであり，不正 Web サイトに使用される IP アドレスが, 特定のネットワークブロックに偏っていることが視覚的に確認できる．この特徴を活用して特徴ベクトル抽出を行い，良性 IP アドレスと悪性 IP アドレスに判別して，Web サイトを分類している．ドメイン名と比べ，IP アドレスは変更が困難であるため，判別に用いる情報として適している．しかし，この手法では特徴を取得する際に利用できる IP アドレスが限られているため，判別が可能な IP アドレスの範囲が狭い．また，IP アドレスを千次元以上の特徴ベクトルに変換して判別に利用しているため判別の負荷が大きい．

2.3 まとめ

本節では，関連研究を踏まえて本研究の位置付けについて述べる．ドメイン名を用いた検出手法では，ドメイン名や URL を用意に且つ頻繁に変更され，ブラックリストから回避される可能性が高いことが問題点としてあげられる．また，IP アドレスを用いた判別手法では，ドメイン名と比較して，容易に情報を変更されにくい．しかし，限られた範囲の特徴を用いているため，悪性の特徴を考慮している IP アドレスの範囲も狭く，判別の負荷が大きいことが問題点としてあげられる．以上の理由により，本研究では，ブラックリストから検出の回避がされにくいとされる不正 Web サイトの特徴を，負荷が小さくなるように未知の不正 Web サイトの判別をできるようにする．

第3章　提案手法

本章では，まず本論文の研究目的とアプローチについて述べ，本論文で使用する用語の定義を行う．次に，アプローチとして用いる不正 Web サイトの特徴分析の結果について述べる．最後に，不正 Web サイトの特徴分析の結果を踏まえて未知の不正 Web サイトの判別手法について説明する．

3.1　研究目的とアプローチ

本研究は，未知の不正 Web サイトを判別するために，未知の Web サイトを正規 Web サイトと不正 Web サイトに判別することを目的とする．アプローチとして，ドメイン名の特徴と IP アドレスの特徴を併用した不正 Web サイトの判別手法を提案する．不正 Web サイトの検出時には，既存手法などで用いられている複数のドメイン名の特徴を検出条件として併用し，検出条件を拡張することで，ブラックリスト型の欠点の解消をめざす．具体的に，用いるドメイン名の検出条件を表 1 に示す．

表 1　ドメイン名の検出条件

Table 1　Detection condition of domain name

検出条件
・10 文字以上の長いドメイン名
・英数字が混在するドメイン名
・マルウェア感染クライアントからアクセスされたドメイン名

ドメイン名の検出条件として，3 つ設定する．1 つ目に，10 文字以上の長いドメイン名を用いる．2 つ目に，英数字が混在するドメイン名を用いる．3 つ目に，マルウェア感染クライアントからアクセスされたドメイン名を用いる．この 3 つの検出条件を用いる理由として，未知の不正 Web サイトの検出の関連研究[11][14][16]で用いられた検出条件の中で，不正 Web サイトの検出率が高精度を示したことが確認されているためである．以上の検出条件を用いることにより，より効率的に不正 Web サイトの検出を行う．

IP アドレスの特徴を用いた判別時には，IP アドレスのすべての範囲において IP アドレスの分布特徴を取得し，従来手法よりも情報量を制限して表現することで，判別コストを軽減しながら高い判別精度の維持をめざす．

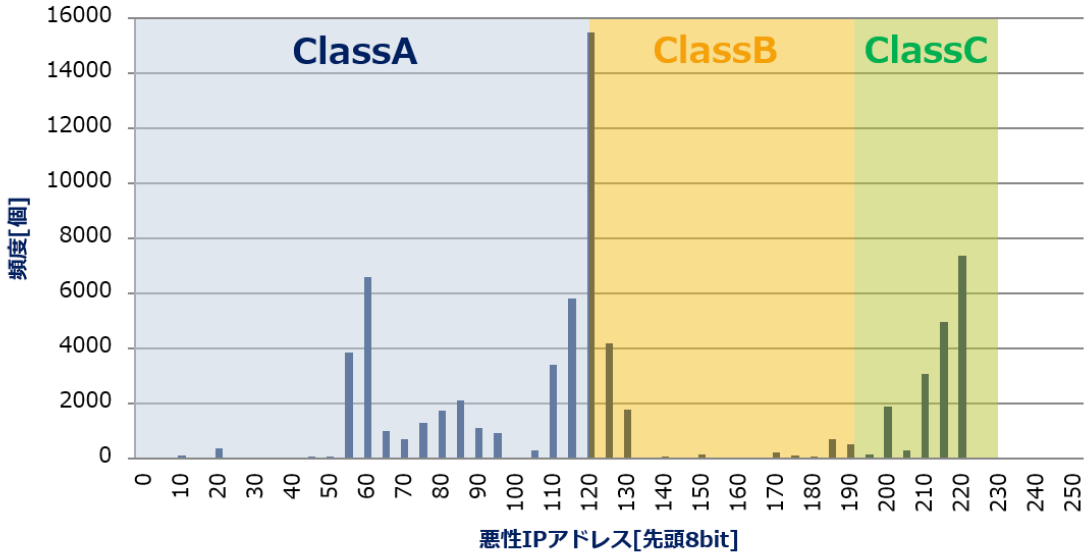


図 4　悪性 IP アドレスの利用頻度

Figure 4　The usage distribution of IP addresses

図 4 は，悪性 IP アドレスの利用頻度を表す分布である．サイバー攻撃は，特定の IP アドレス群を使用する傾向がある[14][15][16]．また，各 IP アドレスクラスにおいて悪性 IP アドレスの利用頻度に差が表れている．文献[15]の研究では，主に IP アドレスクラス C の利用頻度に着目しているが，他の IP アドレスクラスにおいても，特定の悪性 IP アドレス群が集中的に利用されているため，IP アドレスクラス C に限定せず，全ての IP アドレスの範囲の特徴を取得して用いる．また，文献[15][16]では，判別時に，IP アドレスを次の(1)と(2)の式を用いて，最大 1000 以上の次元数に変換した特徴ベクトルを必要としている．

$$\begin{cases} b_k = 1 \ \left(k \ in \ \cup_{n=1}^{N}\{2^8 \cdot (n-1) + X_n\}\right) \\ b_k = 0 \ (otherwise) \end{cases} \quad \cdots(1)$$

$$\begin{cases} b_k = 1 \left(k \ in \ \cup_{n=1}^{N}\{2^8 \cdot (n-1) + X_n\}\right) \\ b_k = 1 \ \left(k \ in \ \cup_{m=N\geq 3}^{N+1}\{2^8 \cdot m + (\sum_{i=1}^{m-1} X_i) mod \ 2^8\}\right) \\ b_k = 0 \ (otherwise) \end{cases} \quad \cdots(2)$$

文献[15][16]で用いられている手法の中で，IP アドレスそのものを 2 進数変換して特徴ベクトルとして用いる手法が一番次元数が少なくコストが抑えられる．そこで， IP アドレスそのものを 2 進数変換したうえで，ネットワークアドレス空間の特徴に基づき，各 IP アドレスのネットワークアドレス部のみを用いることによって，判別に必要な特徴ベクトルの次元数を低コストに抑えた判別を可能にできると考えられる．

以上より，本研究では，未知の Web サイトを検出するためにドメイン名の特徴を活用する．さらに，未知の Web サイトを正規 Web サイトと不正 Web サイトに判別するために IP アドレスの特徴を活用する．

3.2 用語の定義

本節では，本論文で使用する用語の定義を行う．本論文における用語の定義を表 2 に示す.

表 2 用語定義
Table 2 Term definition

用語	定義
IP アドレス	ネットワーク上の機器ひとつひとつに割り振られた識別用の番号である．ネットワーク上の機器（他のコンピュータや，Web サーバーなど）と通信する時は，宛先となる IP アドレスが必要になる．現在主に使われているのは IPv4 と呼ばれる規格の IP アドレスであり，IP アドレスは，コンピュータ内部では 2 進数で処理されることから，32 ビットの整数値で表される．通常は 8 ビットごとに「.」（ピリオド）で区切り，10 進数に直して「192.168.100.34」のように表記する[17].
ドメイン名	IP ネットワークにおいて個々のコンピュータを識別する名称の一部である．インターネット上においては ICANN による一元管理となっており，世界中で絶対に重複しないようになっている．通常，IP アドレスとセットでコンピュータネットワーク上に登録される.
不正 Web サイト	悪質な活動に利用された Web サイトのことである.
正規 Web サイト	正常な Web サイトのことである.
未知の Web サイト（疑惑 Web サイト）	正規 Web サイト・不正 Web サイトのどちらか確認されていない Web サイトのことである.
ブラックリスト	既知の不正 Web サイトの IP アドレスリストのことである.
ホワイトリスト	既知の正規 Web サイトの IP アドレスリストのことである.
悪性 IP アドレス	不正 Web サイトに使用された IP アドレスのことである.
良性 IP アドレス	正規 Web サイトに使用された IP アドレスのことである.
IP アドレスクラス	IP アドレスを A~E の 5 種類に分類した IP アドレスの範囲のことである. IP アドレスの先頭 1~4 ビットまでのビット列の組み合わせによって，どのクラスに属するかを判別することができる．5 つのクラスのうち，ユーザに割り当てられるクラスは A~C の 3 つのみである[17].
検出	未知の Web サイトを発見することである.
判別	未知の Web サイトを正規 Web サイトか不正 Web サイトに分類することである.

用語定義の「IP アドレスクラス」の詳細なクラス分けを表 3 に示す.

表 3　IP アドレスクラス

Table 3　IP address classes

クラス	アドレス範囲	先頭ビットの値
クラス A	0.0.0.0 - 127.255.255.255	ネットワークアドレス長は 8 ビット，ホストアドレス長は 24 ビット
クラス B	128.0.0.0 - 191.255.255.255	ネットワークアドレス長は 16 ビット，ホストアドレス長も 16 ビット
クラス C	192.0.0.0 - 223.255.255.255	ネットワークアドレス長は 24 ビット，ホストアドレス長は 8 ビット
クラス D	224.0.0.0 - 239.255.255.255	IP マルチキャスト専用
クラス E	240.0.0.0 - 255.255.255.255	将来の使用のために予約されている

3.3　システム構成

本節では，提案するシステム構成，未知の Web サイトの検出手法，未知の不正 Web サイト判別手法について述べる．図 5 に，提案システムの概要を示す．

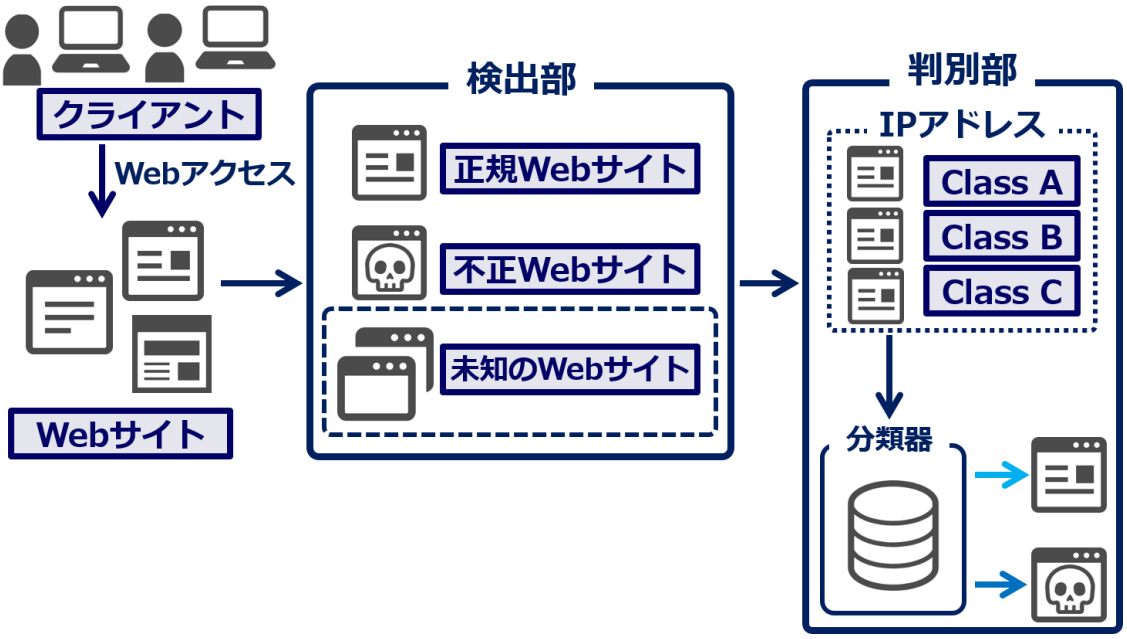


図 5　提案システムの概要

Figure 5　Outline of the proposed system

クライアントがアクセスする Web サイトは，正規 Web サイト，不正 Web サイト，および未知の Web サイトの 3 つに分類できる．このうち，既知である正規 Web サイト・不正 Web サイトに関してはブラックリスト方式で対応可能であるため，未知の Web サイトに重点を置き，IP アドレスのみを用いて低コストで正規・不正に判別可能なシステムを提案する．

図 6 に，提案システムの全体像を示す．

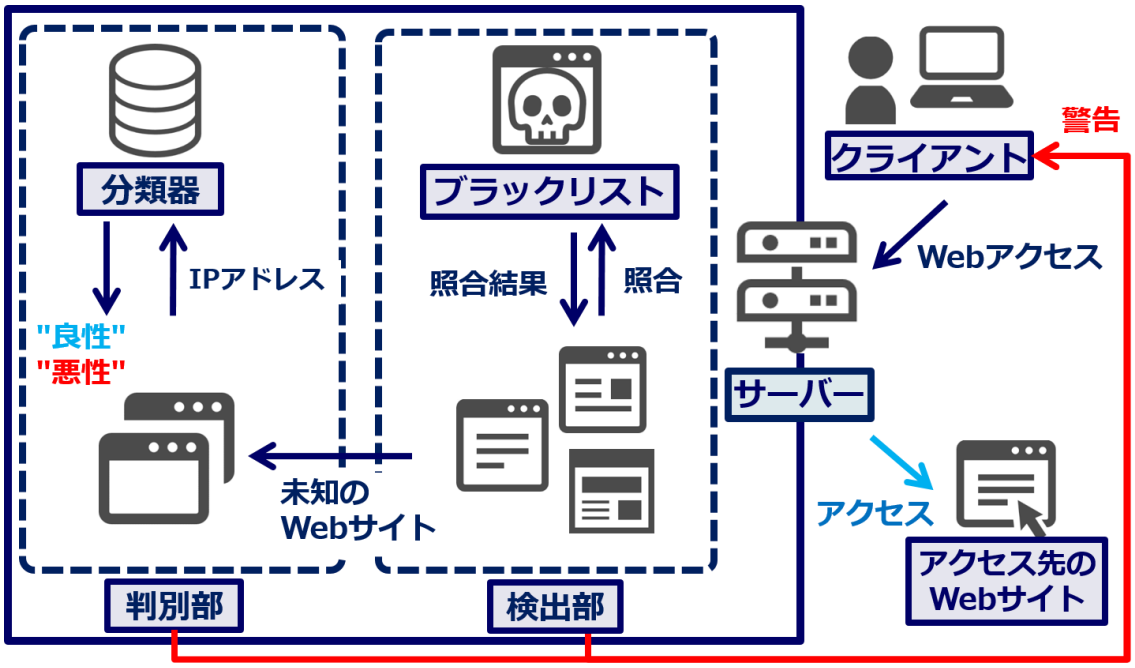


図 6　提案システムの全体像

Figure 6　Overview of the proposed system

提案システムは，検出部と判別部の 2 つのフェーズで構成されている．また，提案システムは，クライアントが DNS サーバーに名前解決のため問い合わせを行い，クライアントに結果を返す通信間に設置する．

検出部では，まず，ドメイン名に関するブラックリストを用いて正規 Web サイトを検出対象から除外し，未知の Web サイトを検出する．クライアントからある Web サイトへ行われる通信が DNS サーバーを通過する際に，検出部は，アクセス先の Web サイトをブラックリストと照合する．アクセス先の Web サイトが未知の Web サイトであると判断された場合，検出部は，判別部に未知の Web サイトの IP アドレスを送信する．判別部は，検出部から送信された IP アドレスを用いて，未知の Web サイトが正規 Web サイトであるか不正 Web サイトであるか判別する．判別結果が正規 Web サイトである場合，クライアントが Web サイトにアクセスすることを許可する．一方，判別結果が不正 Web サイトである場合，クライアントへの警告などによって通信の中断を促し，該当する不正 Web サイトをブラックリストに追加して最新の状態に保つ．

3.4 未知の Web サイトの検出手法

本節では，未知の Web サイトの検出手法について述べる．図 7 は，検出部の詳細を示している．

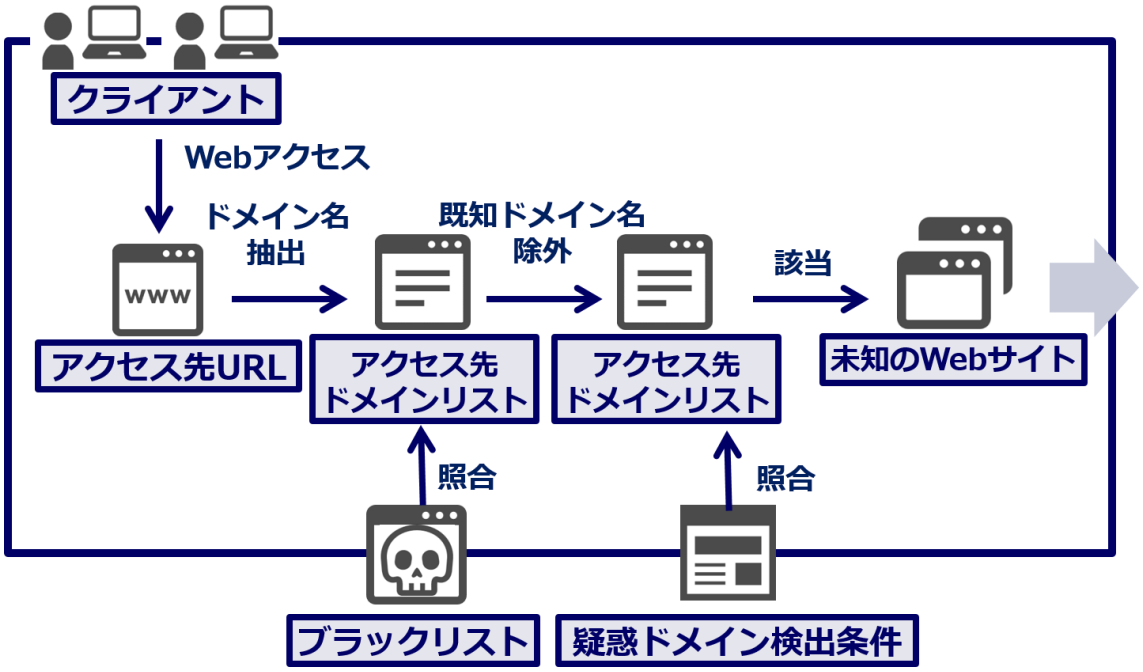


図 7　検出部の詳細

Figure 7　Details of detection unit of unknown Web site

検出部では，ドメイン名の特徴を用いて未知の Web サイトを検出する．Web アクセスされたドメイン名から，Web サイトの URL から取得する．既知の悪性ドメインを除外するために，ドメイン名に関するブラックリストと照合する．ドメイン名がブラックリストに存在しない場合，ドメイン名を，ドメイン名の特徴に基づく検出条件と照合する．ドメイン名の特徴には，10 文字以上のドメイン名，英数字がランダムに混在するドメイン名，マルウェアに感染されたクライアントからアクセスされたドメイン名の 3 つの条件を設定する．

マルウェアに感染したクライアントの検出方法について，図 8 に詳細を示す．

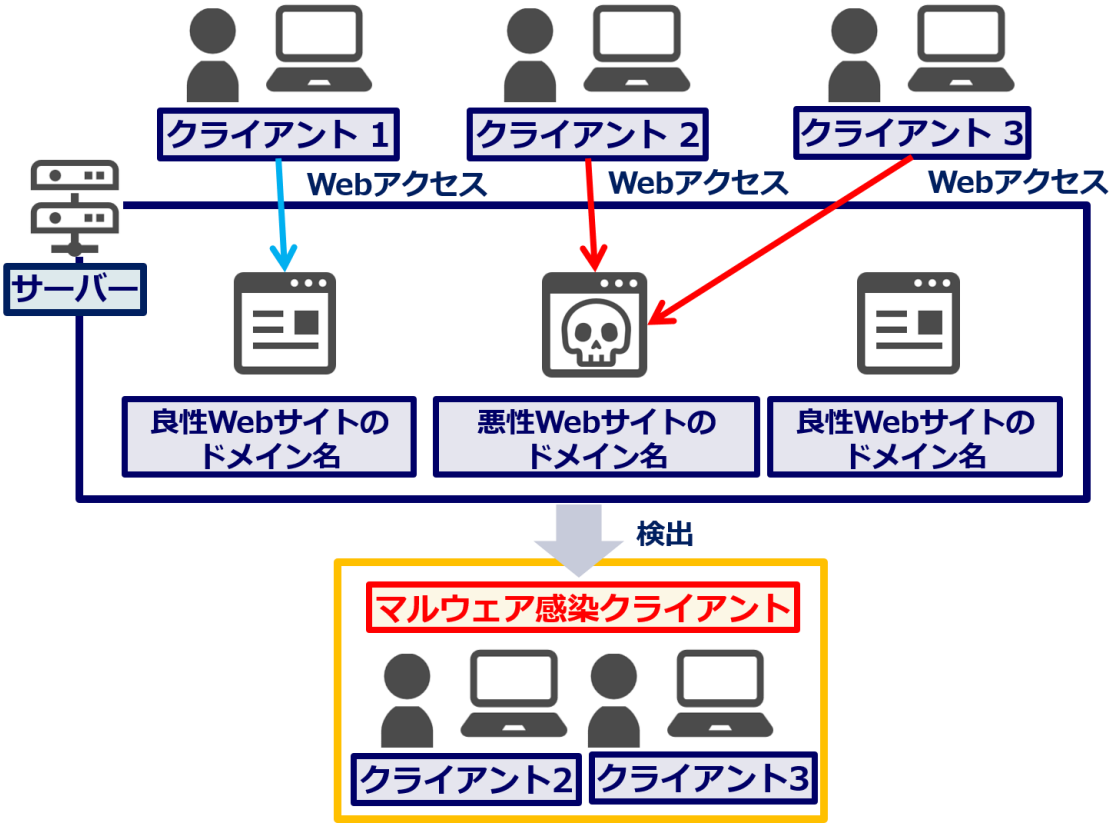


図 8　マルウェアに感染したクライアントの検出方法

Figure 8　Details of detection method of malware infected clients

一般にマルウェアは，感染を拡大させるために多数の不正 Web サイトへアクセスを試みる．そのため，不正 Web サイトは，同時に複数のマルウェア感染クライアントからアクセスが行われている可能性が高い．文献[14]は，悪性のドメイン名を持つ Web サイトにアクセスしているクライアントの検出方法を提案している．検出されたクライアントをマルウェア感染クライアントと呼ぶ．マルウェア感染クライアントが頻繁にアクセスしている Web サイトは，不正 Web サイトであると推定できる．提案方法では，このマルウェア感染クライアントの挙動を確認し，マルウェア感染クライアントがアクセスしている Web サイトのドメインを検出条件に追加して用いることで，既知の不正 Web サイトを特定する．

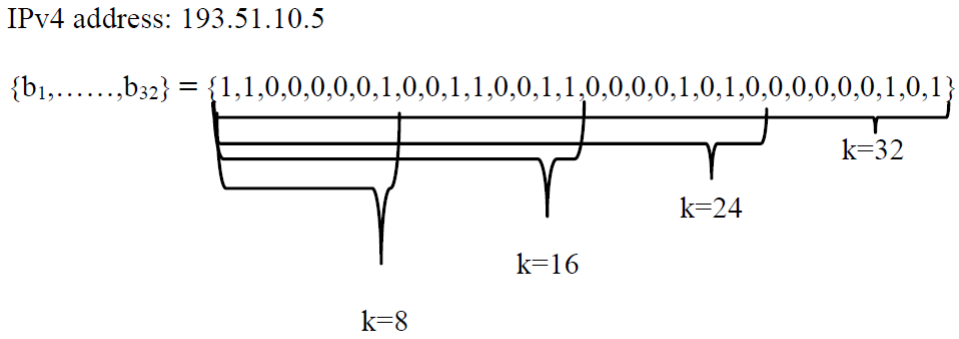
ブラックリスト，ドメイン名の特徴に基づいた検出条件，及びマルウェア感染クライアントのアクセス先のいずれにも該当しない Web サイトを未知の Web サイトと定義し，これらを判別部において正規・不正に判別する対象とする．

3.5　未知の不正 Web サイトの判別手法

本節では，未知の不正 Web サイトの判別方法について述べる．提案システムの判別部は，2 つのフェーズから構成される．既知の不正 Web サイトを蓄積したブラックリストと既知の正規 Web サイトを蓄積したホワイトリストのデータから特徴ベクトルを生成し，それらを教師データとして分類器を構築する．次に，構築された分類器を用いて未知の Web サイトを判別する．

3.5.1 教師データセットを用いた分類器の構築

既知の不正 Web サイトおよび正規 Web サイトの特徴を特徴ベクトル化して，判別のための分類器を生成する．この時の特徴ベクトルの次元数が判別のコストに影響するため，できるだけ次元数を低減した特徴ベクトルを用いて Web サイトを判別する手法を提案する．図 9 に，特徴ベクトルの生成手法を示す．



k	Feature vector
8	b_k=1 (k=1, 2, 8) b_k=0 (otherwise)
16	b_k=1 (k=1, 2, 8, 11, 12, 15, 16) b_k=0 (otherwise)
24	b_k=1 (k=1, 2, 8, 11, 12, 15, 16, 21, 23) b_k=0 (otherwise)
32	b_k=1 (k=1, 2, 8, 11, 12, 15, 16, 21, 23, 30, 32) b_k=0 (otherwise)

図 9　特徴ベクトルの生成

Figure 9　Examples of generating feature vectors

ホワイトリストとブラックリストのデータから構成された教師データセットに含まれるすべての IP アドレスを 2 進数表現のビット列に変換する．すべてのビット列は，k 次元ベクトル$\{b_1, ..., b_k\}$として表される．IP アドレスを表す 32 ビットを，先頭から 8 ビット，16 ビット，24 ビット，32 ビットに分割し，IP アドレスクラスに応じて特徴ベクトルを生成する．IP アドレスクラス A の場合は，先頭 8 ビットを用いて，8 次元の特徴ベクトルを生成する．IP アドレスクラス B の場合は，先頭 16 ビットを用いて，16 次元の特徴ベクトルを生成する．IP アドレスクラス C の場合は，先頭から 24 ビットを用いて，24 次元の特徴ベクトルを生成する．悪性 IP アドレスから生成された特徴ベクトルには「1」，良性 IP アドレスから生成された特徴ベクトルには「0」とラベルを付ける．表 4 は，教師データセットの特徴ベクトルにラベルを付ける例を示している．

表 4　教師データセットの例

Table 4　Examples of labeling feature vectors of training datasets

IP address	Feature vector	Label
192.51.10.5	1,1,0,0,0,0,0,0,0,0,1,1,0,0,1,1	1
10.10.10.10	0,0,0,0,1,0,1,0	1
203.4.12.89	1,1,0,0,1,0,1,1,0,0,0,0,0,1,0,0,0,0,0,0,1,1,0,0	0
…	…	…

本稿では，パターン識別法の 1 つである SVM（Support Vector Machine）を用いた判別を行っている．文献[10]は，SVM を用いることにより，不正 Web サイトの高精度な検出が可能であることを示している．また，頻繁に特徴が更新される場合は，オンライン学習を用いる手法も考えられる．その中の識別法の 1 つとして，オンライン SVM がある．オンライン学習を用いることで学習データの時間変化に追随することが可能であり，学習に用いるデータの時間方向の変化が想定される場合，有望な方式である．しかしながら，我々が用いているデータは一年単位で公開されるものであるため，データの更新に合わせた再学習の頻度は高々年に数回と想定され，バッチ型の SVM アルゴリズムでも十分であると判断した．今後，細粒度で更新データが入手できる環境で本提案手法を用いる場合にはオンライン SVM 等の手法を検討する価値があると思われる．

上記のように，各 IP アドレスクラスごとに，次元の異なる特徴ベクトルに基づいた分類器を構築する．

3.5.2 分類器を用いた未知の IP アドレスの判別

検出部から渡された未知 Web サイトの IP アドレスは，3.5.1 節で構築された分類器によって良性と悪性に判別される．図 10 に，判別手法の概要を示す．

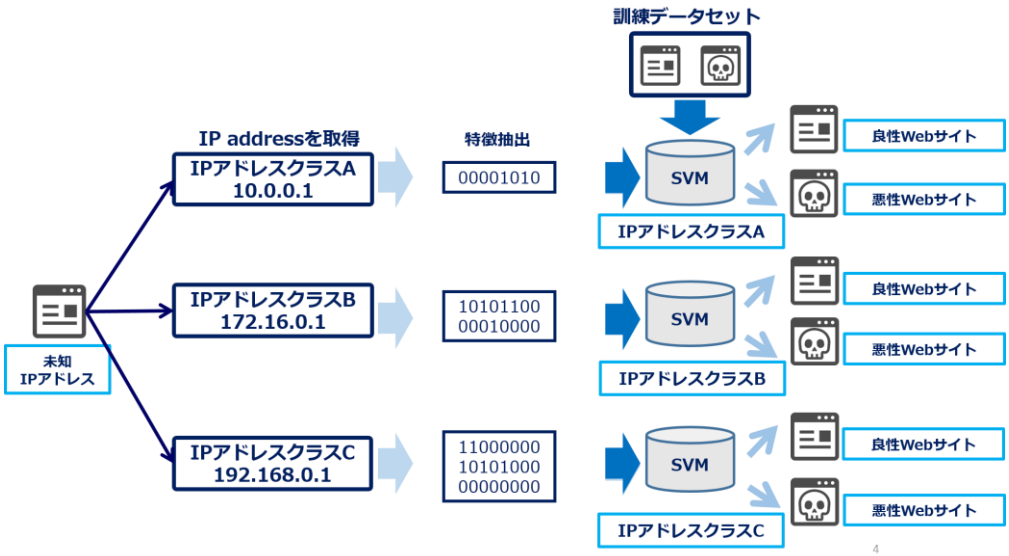


図 10　判別手法

Figure 10　Classification process

判別部は, 検出部から渡された IP アドレスから特徴ベクトルを生成する. この特徴ベクトルを, 判別部の 3.5.1 節で構築された分類器によって良性，または悪性に判別する．最後に，既知の IP アドレスと，判別を完了した IP アドレスを教師データとして追加し，分類器の更新を行う．図 11 に，分類器の学習について詳細を示す.

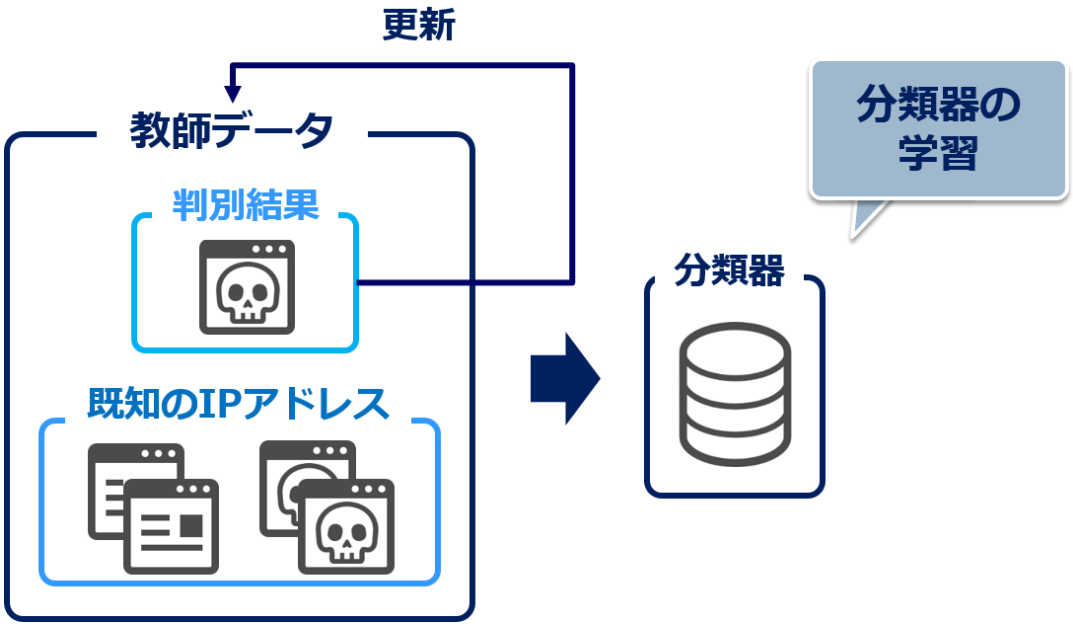


図 11　分類器の学習

Figure 11　Learning of classifiers

最新の悪性アドレス分布特徴を反映した分類器を用いることで，Web サイトに対する判別精度が向上できると考えられる．

これらの提案手法を実現するためには，教師データとして用いるデータセットを判別に適した状態にする必要がある．そこで，教師データセットの元となるブラックリストから取得できる特徴を分析する必要がある．通常のブラックリストを用いた判別は，基本的に既知の悪性 IP アドレスによる通信を遮断することになり，既知の攻撃に対しては有効であるものの，未知の IP アドレスからの攻撃については対処困難である．ブラックリストを用いた判別は，以下の 3 つのパターンが考えられる．

1) ベースラインとしてブラックリストそのものを用いた分類器
2) ブラックリスト全体を用い，時間的な変化を想定しない分類器
3) ブラックリストの時間的な変化に応じて再学習を行った分類器

ブラックリストに含まれる IP アドレスの時間的な変化に対して, 対応可能かどうかを確認するため，教師データとして用いられる IP アドレスを分析する．

3.6 ブラックリストにおける出現 IP アドレス分布の時間的な変化

本節では，ブラックリストにおける出現 IP アドレス分布の時間的な変化について述べる．ブラックリストが時間的に変化するのかを調査するため，悪性 IP アドレス利用頻度のデータを元に，IP アドレスクラスの利用状況を分析した．図 12 に，CCC DATAset[18]から収集した IP アドレス数が比較的多い 2008 年から 2011 年を対象に悪性 IP アドレスの利用頻度をグラフ化したものを示す．

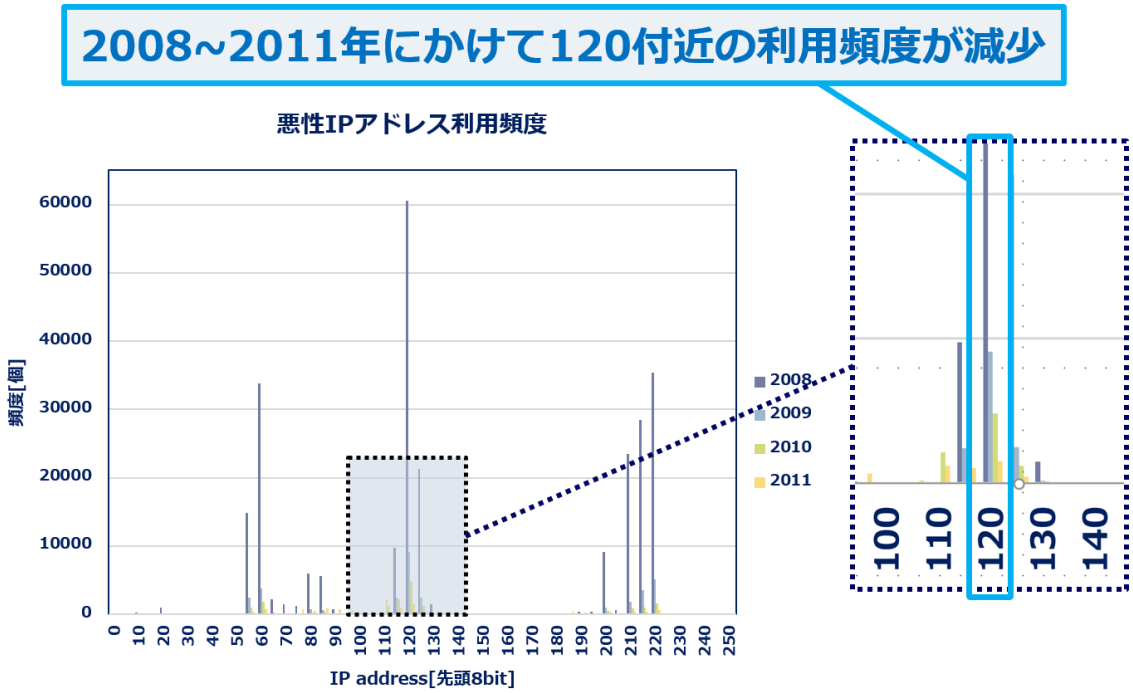


図 12　IP アドレス分布 (IP アドレス上位 8 ビットの 120 付近拡大)[2008-2011]

Figure 12　Usage frequency of malicious IP addresses (Enlargement of the first 8 bits of IP address near 120) [2008-2011]

図 12 は，IP アドレス上位 8 ビットの 120 付近に着目し拡大したものである．2008 年の 120 付近の悪性 IP アドレス数は，60,579 個であった．一方，2009 年の 120 付近の悪性 IP アドレス数は，9,084 個であり，2008 年の悪性 IP アドレス数より数が減少したことが確認された．また，2010 年の 120 付近の悪性 IP アドレス数は，4,819 個であった．2008 年，2009 年の悪性 IP アドレス数より数が減少していることが確認された．2011 年の 120 付近の悪性 IP アドレスは，1,516 個であり，2008 年，2009 年，2010 年の悪性 IP アドレス数よりもさらに数が減少したことが確認された．したがって，これらの結果から，2008 年から 2011 年にかけて悪性 IP アドレスの利用頻度が減少していることが確認された．

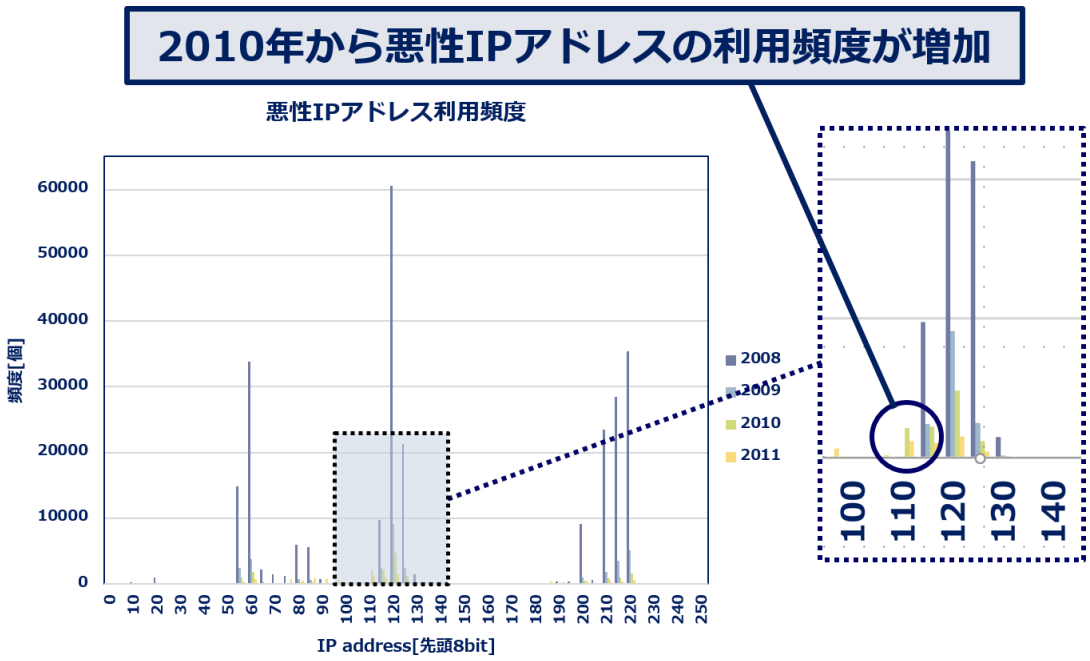


図 13　IP アドレス分布(IP アドレス上位 8 ビットの 110 付近拡大)[2008-2011]

Figure 13　Usage frequency of malicious IP addresses (Enlargement of the first 8 bits of IP address near 110) [2008-2011]

次に，IP アドレス上位 8 ビットの 110 付近に着目する．図 13 は，IP アドレス上位 8 ビットの 110 付近に着目し拡大したものである．2008 年の 110 付近の悪性 IP アドレス数は，0 個であった．また，2009 年の 110 付近の悪性 IP アドレス数も 0 個であった．一方，2010 年の 110 付近の悪性 IP アドレス数は，2,135 個であり．2008 年，2009 年の悪性 IP アドレス数より増加したことが確認された. 2011 年の 110 付近の悪性 IP アドレス数は, 1,182 個であった. したがって, これらの結果から, 2008 年から 2009 年まで悪性 IP アドレスの利用頻度が 0 件であるのに対し, 2010 年から利用頻度が増加していることが確認された.

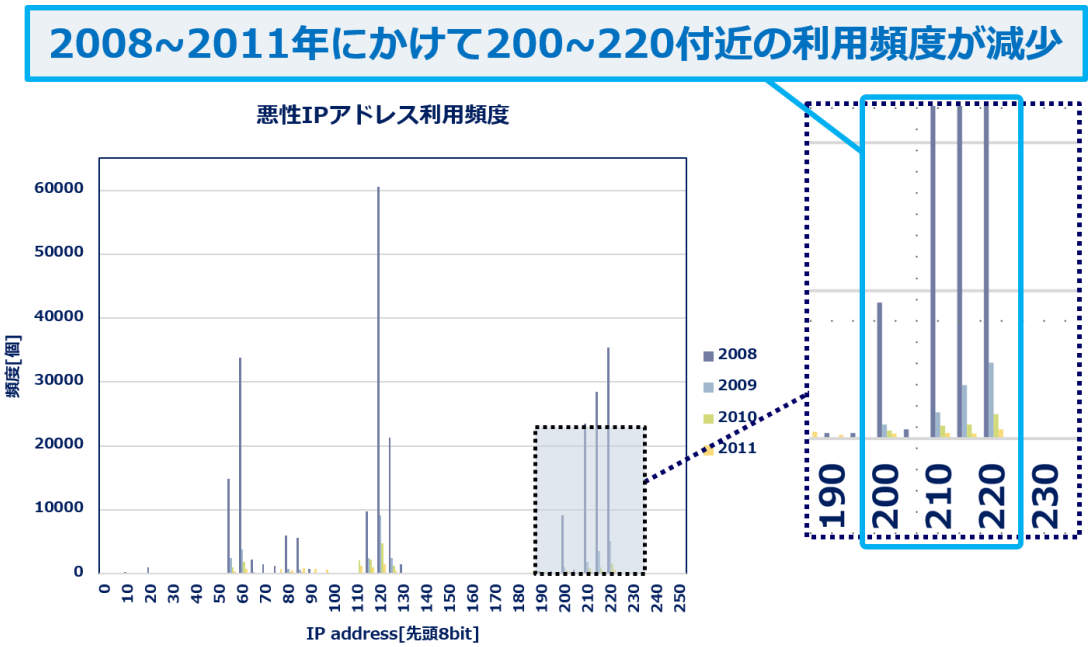


図 14　IP アドレス分布(IP アドレス上位 8 ビットの 200~220 付近拡大)[2008-2011]

Figure 14　Usage frequency of malicious IP addresses (Enlargement of the first 8 bits of IP address near 200 to 220) [2008-2011]

さらに，IP アドレス上位 8 ビットの 200 から 220 付近に着目する．図 14 は，IP アドレス上位 8 ビットの 200 から 220 付近を拡大したものである．まず，IP アドレス上位 8 ビットの 200 付近について分析した．2008 年の 200 付近の悪性 IP アドレス数は，9,192 個であった．一方，2009 年の 200 付近の悪性 IP アドレス数は，941 個であり，2008 年の悪性 IP アドレス数より減少したことが確認された．また，2010 年の 200 付近の悪性 IP アドレス数は，529 個であり，2008 年，2009 年の悪性 IP アドレス数より減少していることが確認された．2011 年の 200 付近の悪性 IP アドレスは，352 個であり，2008 年，2009 年，2010 年の悪性 IP アドレス数よりもさらに減少したことが確認された．次に，IP アドレス上位 8 ビットの 210 付近について分析した．2008 年の 210 付近の悪性 IP アドレス数は，23,435 個であった．一方，2008 年の 200 付近の悪性 IP アドレス数は，1,782 個であり，2009 年の悪性 IP アドレス数より減少したことが確認された．また，2010 年の 210 付近の悪性 IP アドレス数は，854 個であり，2008 年，2009 年の悪性 IP アドレス数より減少していることが確認された． 2011 年の 210 付近の悪性 IP アドレスは，365 個であり，2008 年，2009 年，2010 年の悪性 IP アドレス数よりもさらに減少したことが確認された．最後に，IP アドレス上位 8 ビットの 220 付近について分析した．2008 年の 210 付近の悪性 IP アドレス数は，35,362 個であった．一方，2009 年の 200 付近の悪性 IP アドレス数は，5,121 個であり，2009 年の悪性 IP アドレス数より減少したことが確認された．また，2010 年の 210 付近の悪性 IP アドレス数は，1,626 個であり，2008 年，2009 年の悪性 IP アドレス数より減少していることが確認された．2011 年の 210 付近の悪性 IP アドレスは，628 個であり，2008 年，2009 年，2010 年の悪性 IP アドレス数よりもさらに減少したことが確認された．したがって，これらの結果から，2008 年から 2011 年にかけて悪性 IP アドレスの利用頻度が減少していることが確認された．

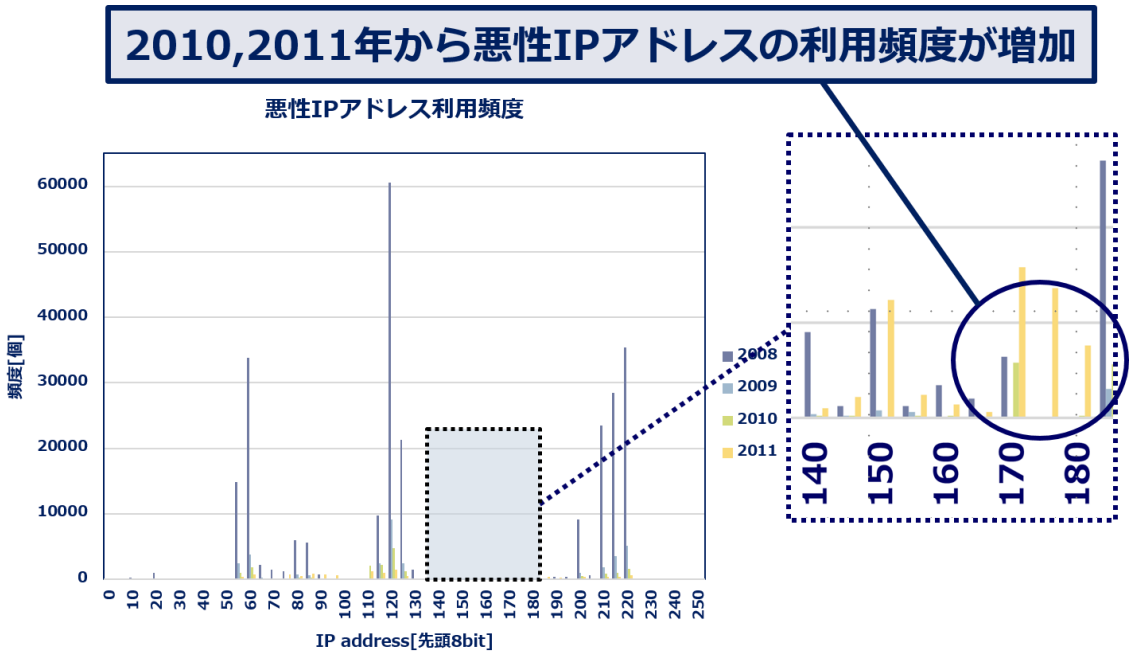


図 15　IP アドレス分布 (IP アドレス上位 8 ビットの 170~180 付近拡大)[2008-2011]

Figure 15　Usage frequency of malicious IP addresses (Enlargement of the first 8 bits of IP address near 170 to 180)[2008-2011]

最後，IP アドレス上位 8 ビットの 170~180 付近に着目する．図 15 は，IP アドレス上位 8 ビットの 170 から 180 付近を拡大したものである．まず，IP アドレス上位 8 ビットの 170 付近について分析した．2008 年の 170 付近の悪性 IP アドレス数は，32 個であった．また，2009 年の 170 付近の悪性 IP アドレス数は 0 個であり，2008 年の悪性 IP アドレス数よりも減少した．一方，2010 年の 170 付近の悪性 IP アドレス数は，29 個であり，2009 年の悪性 IP アドレス数より増加したことが確認された．また，2011 年の 170 付近の悪性 IP アドレス数は，79 個であり，2009 年，2010 年の悪性 IP アドレス数より増加したことが確認された．次に，IP アドレス上位 8 ビットの 180 付近について分析した．2008 年の 180 付近の悪性 IP アドレス数は，0 個であった．また，2009 年の 180 付近の悪性 IP アドレス数も 0 個であった．一方，2010 年の 180 付近の悪性 IP アドレス数は，1 個であり，2008 年，2009 年の悪性 IP アドレス数より増加したことが確認された．また，2011 年の 180 付近の悪性 IP アドレス数は，38 個であり，2009 年，2010 年の悪性 IP アドレス数より増加したことが確認された．したがって，これらの結果から，2008 年から 2009 年まで悪性 IP アドレスの利用頻度が低い状況であるのに対し，2010 年から利用頻度が増加していることが確認された．

悪性 IP アドレス利用頻度のデータを元に，IP アドレスクラスの利用状況を分析した結果，全体的に利用頻度に変化が生じていると考えられる．したがって，各 IP アドレスクラスの判別を年度別に行うことにより，年度別に異なる特徴を生かすことができると考えられる．そこで，本実験では，教師データを年度別に作成して分類器を学習させることにする．

第4章　評価・考察

本章では，まず，提案手法の有効性を確認するための評価方法について述べる．次に，３パターン方法の評価実験とそれらの結果について述べ，最後に，考察について述べる．

4.1　評価実験の概要

本節では, 3.6 節の結果から悪性 IP アドレスの利用における経年変化が認められることから，それが判別性能に与える影響を把握し，最適な判別器の構成を決定するために以下の実験を行う．まず，評価指標について述べる．次に，データセットついて述べる．最後に，システムの実装環境について述べる．

4.1.1　評価指標

提案手法の有効性を確認するために, 判別部の 3.5.1 節で構築された分類器を精度, 適合率, 再現率の 3 つを評価指標と定義して評価した．本稿では，悪性 IP アドレスを正しく悪性 IP アドレスと判別した数を表す真陽性（TP），良性 IP アドレスを誤って悪性 IP アドレスと判別した数を偽陽性（FP），良性 IP アドレスを正しく良性 IP アドレスと判別した数を真陰性（FN），悪性 IP アドレスを誤って良性 IP アドレスと判別した数を偽陰性（TN）とする．このときの精度，適合率，再現率をそれぞれ下記の計算式(1)(2)(3)で求める．

$$精度 = (TP + TN)/(TP+ TN + FP+FN) \quad \cdots(1)$$
$$適合率 = TP/(TP+ FP) \quad \cdots(2)$$
$$再現率 = TP/(TP+ FN) \quad \cdots(3)$$

悪性データセットは, Malware Workshop Datasets[18]から取得した IP アドレスを用いている．悪性 IP アドレスと良性 IP アドレスの比率は 8 : 2，5 : 5，2 : 8 の 3 パターンを作成した．悪性 IP アドレスの教師データセットは，マルウェア検体を収録したボット観測データ群 CCC DATAsets（2008 年～2011 年）と Web 感染型マルウェアデータ D3M（2010 年～2015 年）のデータをもとに作成した. また, 良性 IP アドレスの教師データセットは, Alexa Top Global Sites[19]の 50,000 件（2016）のデータとホワイトデータセット NCD in MWS Cup(2014)のデータをもとに作成した．

前節でブラックリストに経年変化が確認された．これが分類精度に与える影響を検討するため，3.5.2 節に述べた 3 通りの分類器 (ベースラインとしてブラックリストそのものを用いた分類器，ブラックリスト全体を用い，時間的な変化を想定しない分類器，ブラックリストの時間的な変化に応じて再学習を行った分類器)を構成して精度を比較する実験を行う．評価は，各 IP アドレスの上位 8,16,24,32 ビットごとに行う．教師データとテストデータは，上記に述べたデータセットの IP アドレスからランダムに分割した．

4.1.2 良性データ

Alexa Top Global Sites(Alexa)は，Web サイトのアクセス数の調査や統計をとっている．Alexa では，世界，国別のカテゴリでそれぞれアクセス数が高い Web サイト上位 500 件のランキングを公表している[19]. また, Web コンテンツのカテゴリ別で, それぞれのアクセス数が高い Web サイト最大上位 500 件を公表しているため，正規 Web サイトの IP アドレスとして利用できると考えた．

本研究では, Alexa が公表する Web サイトから良性 IP アドレスデータを抽出してホワイトリストを構成する．

4.1.3 悪性データ

NTT セキュアプラットフォーム研究所は，Web クライアント型ハニーポットを使用し，ドライブバイダウンロード攻撃に関連するデータを収集している[18]．NTT セキュアプラットフォーム研究所は 2010 年からドライブバイダウンロード攻撃に関するデータを収集しており, 感染手法の検知，解析技術の研究のためにドライブバイダウンロード攻撃に関するデータ D3M(Drive-by Download Data by Marionette)2014 データセットを研究機関に提供している．D3M2014 データセットには NTT セキュアプラットフォーム研究所が過去に収集した通信データセット D3M2010，D3M2011，D3M2012，D3M2013 が含まれる．

本実験では，D3M データセットの通信データから，悪性 IP アドレスデータを抽出してブラックリストを構成する．ブラックリストを構成する際には，クライアント側の IP アドレスと DNS に問い合わせが行われた IP アドレスを除外して利用する．このとき，悪性 IP アドレスのブラックリストから，DNS に問い合わせが行なわれた IP アドレスを除外しているのは，DNS を介している通信に正規 Web サイトが含まれるためである．

4.1.4 実装環境

実験は IP アドレスからバイナリビット列に変換して，抽出した特徴ベクトルに，良性・悪性を示すラベルを付け，CSV ファイル形式で使用する．SVM は，プログラミング言語 python で実装した．実験環境を表 5 に示す．

表 5　実装環境

Table 5　Implementation environment

ハードウェア（PC）	
OS	Windows 10
CPU	Intel Core i3-3110M 2.40GHz
RAM	4.00 GB
SVM	
機能	Scikit-learn
言語	Python 2.7

4.2 評価実験 1：ブラックリストを用いた検出

本節では，評価実験 1 の概要と実験結果について述べる．評価実験 1 では，ブラックリストを用いて不正 Web サイトの検出を行う．評価実験 1 の目的は，ベースラインとしてブラックリストそのものを用いた分類器の判別性能を確認することである．まず，データセットについて説明する．実験で用いるブラックリストは，データ群から取得できる悪性 IP アドレスを用いてランダムに 5 つ作成した．ブラックリストは，1 セットあたり 17,000 個程度使用した．テストデータは, ブラックリストとホワイトリストから取得できる IP アドレスを用いてランダムに 5 つ作成した．テストデータは，1 セットあたり 20,000 個使用した．作成されたテストデータセットは，良性と悪性の割合を 8:2 とする．評価実験 1 に用いた IP アドレス数を，表 6 に示す．次に，分類器について説明する．評価実験 1 の詳細を図 16 に示す．

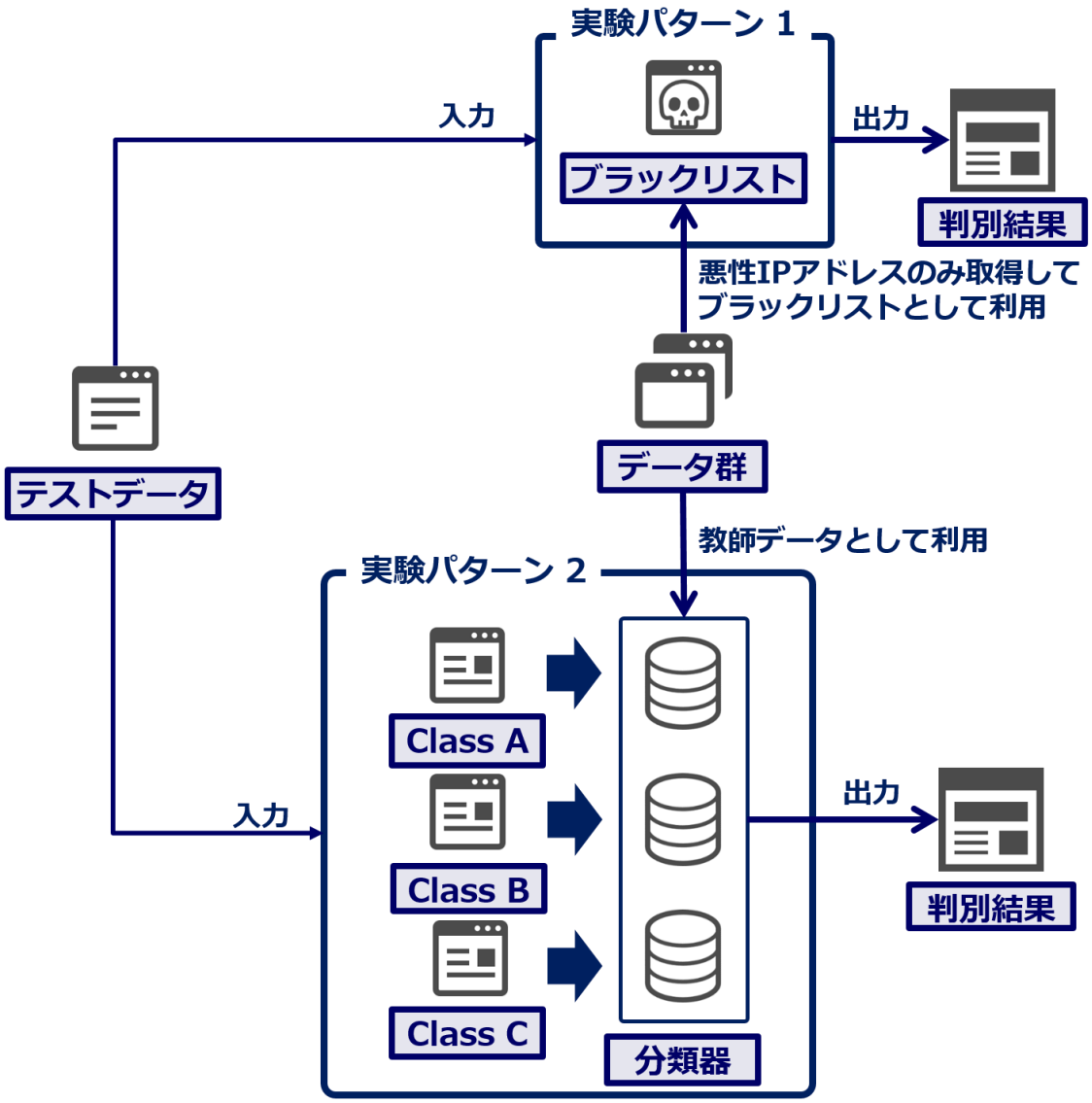


図 16 評価実験 1 の詳細

Figure 16 The overview of evaluation experiment 1

分類器は 2 パターン作成する．一つ目は，ブラックリストの IP アドレス 32bit 全て用いて分類器とする．テストデータと照合し，一致する IP アドレスの精度を算出する．この工程を 5 つのテストデータで行い，平均値を取る．二つ目は，一つ目のパターンと同じデータ群を用いる．データ群を教師データとして用いることで，機械学習した分類器を構築する．テストデータを入力すると，システム内部で IP アドレスクラスごとに分類が行われ，判別結果を出力する．5 分割交差検定により，テストデータごとに判別精度を算出する．この工程を 5 つのテストデータで行い，平均値を取る．以上の 2 パターンの分類器の判別精度を比較し評価する．評価実験 1 に用いた IP アドレス数を，表 6 に示す.

表 6　評価実験 1 の IP アドレス数

Table 6　The number of IP addresses used in evaluation experiment 1

	悪性 IP アドレス数	良性 IP アドレス数
ブラックリスト	322,687	
ホワイトリスト		538,156

4.2.1　実験結果

評価実験 1 の結果について述べる. ブラックリストを用いた悪性 IP アドレスの検出結果を評価した．ブラックリストの検出結果として，真陽性，偽陽性，真陰性，偽陰性を表 7 に示す.

表 7　ブラックリストを用いた検出結果

Table 7　Detection result using blacklist

	真陽性	偽陰性	真陰性	偽陽性
テストデータ 1	878	16,300	2,822	0
テストデータ 2	891	16,291	2,818	0
テストデータ 3	912	16,279	2,809	0
テストデータ 4	916	16,133	2,951	0
テストデータ 5	921	16,235	2,844	0

次に，ブラックリストの検出結果として，精度，適合率，再現率を表 8 に示す.

表 8　ブラックリストを用いた検出結果 (%)

Table 8　Detection result using blacklist（%）

	精度	適合率	再現率
テストデータ 1	18.5	5.111	100
テストデータ 2	18.545	5.185	100
テストデータ 3	18.605	5.305	100
テストデータ 4	19.335	5.372	100
テストデータ 5	18.825	5.368	100
平均	18.762	5.268	100

精度は平均 18.762%，適合率は 5.27%，再現率は 100%を示した．したがって，ブラックリストを用いた悪性 IP アドレスの検出では，十分に検出できない結果となった.

次に，IP アドレスクラス別の判別結果として，真陽性，偽陽性，真陰性，偽陰性を表 9 に示す.

表 9　IP アドレスクラス別の判別結果の平均

Table 9　Average of classification results of each IP address class

	真陽性	偽陰性	真陰性	偽陽性
テストデータ 1	14,882	2,314	1,507	1,297
テストデータ 2	14,828	2,337	1,506	1,329
テストデータ 3	14,764	2,368	1,540	1,328
テストデータ 4	14,959	2,286	1,346	1,346
テストデータ 5	14,805	2,322	1,542	1,331

IP アドレスクラス別の判別結果として，精度，適合率，再現率を表 10 に示す.

表 10　IP アドレスクラス別の判別結果の平均 (%)

Table 10　Average of classification results of each IP address class (%)

	精度	適合率	再現率
テストデータ 1	81.945	86.543	91.983
テストデータ 2	81.670	86.385	91.774
テストデータ 3	81.520	86.177	91.747
テストデータ 4	81.782	86.743	91.744
テストデータ 5	81.735	86.442	91.751
平均	81.730	86.458	91.800

ブラックリストを用いた検出結果と比較すると, 精度, 適合率は 80%以上を示し, 再現率は 90%以上を示し，高い数値が得られた．したがって，IP アドレスクラス別の判別の方が 80%程度で判別できることがわかった.

4.3　評価実験 2：各 IP アドレスクラスを用いた判別

本節では，評価実験 2 の概要と実験結果について述べる．評価実験 2 では，IP アドレスクラスごとに分けた判別を行う．評価実験 2 の目的は，ブラックリスト全体を用い，時間的な変化を想定しない分類器の判別性能を確認することである．そのため，評価実験 2 では，取得できる全ての IP アドレスを用いてデータセットを作成する．実験は，IP アドレスのネットワークアドレス部の特徴を用いて Web サイトの判別に対する有効性を評価する．具体的には，IP アドレスクラス A，B，C に属する各 IP アドレスについて，それぞれの IP アドレスクラスのネットワークアドレス部を示す上位 8 ビット，16 ビット，24 ビット部分を特徴ベクトルとして用いて判別したときの精度で評価する．手順として，まず，教師データによって生成された分類器を持つ提案システムに，テストデータセットを入力し，判別結果を取得する．次に，交差検定により，判別精度を算出する．最後に，入力に用いた各ビット数特徴ベクトルごとの判別精度を比較し評価する．評価実験 2 に用いた IP アドレス数を，表 11 に示す.

表 11　評価実験 2 の IP アドレス数

Table 11　The number of IP addresses used in evaluation experiment 2

	悪性 IP アドレス数	良性 IP アドレス数
IP アドレスクラス A	49,164	40,667
IP アドレスクラス B	3,523	10,735
IP アドレスクラス C	75,000	14,288

4.3.1　実験結果

評価実験 2 の結果について述べる．IP アドレスのうち判別に用いる部分として，Case1 を上位 8 ビット，Case2 を上位 16 ビット，Case３を上位 24 ビット，Case4 を上位 32 ビットと定義し，それぞれの場合について判別結果を評価した．まず，IP アドレスクラス A の実験結果として，真陽性，偽陽性，真陰性，偽陰性を表 12 に示す.

表 12　IP アドレスクラス A の実験結果

Table 12　The experimental result of IP address of Class A

	真陽性	偽陰性	真陰性	偽陽性
Case1(k=8)	29,363	3,171	4,822	3,311
Case2(k=16)	29,246	3,288	4,810	3,323
Case3(k=24)	29,245	3,289	4,818	3,315
Case4(k=32)	29,244	3,290	4,867	3,266

次に，IP アドレスクラス A の判別結果を表 13 に示す.

表 13　IP アドレスクラス A の実験結果（%）

Table 13　The experimental result of IP address of Class A（%）

	精度	適合率	再現率
Case1(k=8)	84.06079	89.86656	90.25327
Case2(k=16)	83.74358	89.79705	89.89365
Case3(k=24)	83.76079	89.8188	89.89058
Case4(k=32)	83.87882	89.95386	89.8875

精度と再現率は IP アドレスクラス A のネットワークアドレス部のみを特徴ベクトルとして用いた Case1 で最高値を示した．適合率は，Case4 で最高値を示した．Case1 で正しく悪性 IP アドレスであると分類できた数に着目すると，29,363 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 3,171 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，4,822 個であった．そのうち，誤って良性 IP アドレスを分類した数が 3,311 個であった. Case2 で正しく悪性 IP アドレスであると分類できた数に着目すると，29,246 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 3,288 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，4,810 個であった．そのうち，誤って良性 IP アドレスを分類した数が 3,323 個であった．Case3 で正しく悪性 IP アドレスであると分類できた数に着目すると，29,245 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 3,289 個であった．また，正しく良性 IP アドレスである

と分類できた数に着目すると，4,818 個であった．そのうち，誤って良性 IP アドレスを分類した数が 3,266 個であった．Case4 で正しく悪性 IP アドレスであると分類できた数に着目すると，29,244 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 3,290 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，4,867 個であった．そのうち，誤って良性 IP アドレスを分類した数が 3,266 個であった．関連研究[15]の精度が 74.7~75.1%であったのに対し，提案手法の精度は 84%であり，関連研究の精度を上回る結果が得られた．したがって，ネットワークアドレス部を用いた判別は有効であると考えられる．

次に，IP アドレスクラス B の実験結果を示す．IP アドレスクラス B の実験結果として，真陽性，偽陽性，真陰性，偽陰性を表 14 に示す．

表 14　IP アドレスクラス B の実験結果

Table 14　The experimental result of IP address of Class B

	真陽性	偽陰性	真陰性	偽陽性
Case1(k=8)	2,597	221	347	359
Case2(k=16)	2,510	308	369	337
Case3(k=24)	2,544	274	379	327
Case4(k=32)	2,551	267	383	323

IP アドレスクラス B の実験結果を表 15 に示す.

表 15　IP アドレスクラス B の実験結果（%）

Table 15　The experimental result of IP address of Class B（%）

	精度	適合率	再現率
Case1(k=8)	83.54143	87.85521	92.15756
Case2(k=16)	81.69694	88.16298	89.07026
Case3(k=24)	82.94552	88.61024	90.27679
Case4(k=32)	83.25766	88.76131	90.5252

精度と再現率は，Case1 で最高値を示した．一方，適合率は，Case4 で最高値を示した．Case1 で正しく悪性 IP アドレスであると分類できた数に着目すると, 2,597 個であった. そのうち，誤って悪性 IP アドレスを分類した数が 221 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，347 個であった．そのうち，誤って良性 IP アドレスを分類した数が 359 個であった．Case2 で正しく悪性 IP アドレスであると分類できた数に着目すると，2,510 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 308 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，369 個であった．そのうち，誤って良性 IP アドレスを分類した数が 337 個であった．Case3 で正しく悪性 IP アドレスであると分類できた数に着目すると，2,544 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 274 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，379 個であった．そのうち，誤って良性 IP アドレスを分類した数が 327 個であった. Case4 で正しく悪性 IP アドレスであると分類できた数に着目すると，2,551 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 267 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，383 個であった．

そのうち，誤って良性 IP アドレスを分類した数が 323 個であった．これらの結果から，IP アドレスクラス B のネットワークアドレス部のみを特徴ベクトルとして用いた Case2 で最高値を達成することができていない状態である．また，関連研究[15]の精度が 84.6~86.2%であったのに対し，提案手法の精度は 81.6~83.5%であり，関連研究の精度を下回る結果が得られた．

最後に，IP アドレスクラス C の実験結果について述べる．IP アドレスクラス C の実験結果として，真陽性，偽陽性，真陰性，偽陰性を表 16 に示す．

表 16　IP アドレスクラスＣの実験結果

Table 16　The experimental result of IP address of Class C

	真陽性	偽陰性	真陰性	偽陽性
Case1(k=8)	10,347	1,083	1,338	1,520
Case2(k=16)	10,283	1,147	1,319	1,539
Case3(k=24)	10,287	1,143	1,321	1,537
Case4(k=32)	10,354	1,076	1,251	1,607

IP アドレスクラス C の実験結果を表 17 に示す．

表 17　IP アドレスクラス C の実験結果（%）

Table 17　The experimental result of IP address of Class C（%）

	精度	適合率	再現率
Case1(k=8)	81.78191	87.19137	90.52493
Case2(k=16)	81.20101	86.9819	89.965
Case3(k=24)	81.243	87.00101	90.0
Case4(k=32)	81.222	86.56467	90.58618

精度と適合率は，Case1 で最高値を示した．一方，再現率は，Case4 で最高値を示した．Case1 で正しく悪性 IP アドレスであると分類できた数に着目すると，10,347 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 1,083 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，1,338 個であった．そのうち，誤って良性 IP アドレスを分類した数が 1,520 個であった．Case2 で正しく悪性 IP アドレスであると分類できた数に着目すると，10,283 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 1,147 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，1,319 個であった．そのうち，誤って良性 IP アドレスを分類した数が 1,539 個であった．Case3 で正しく悪性 IP アドレスであると分類できた数に着目すると，10,287 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 1,143 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，1,321 個であった．そのうち，誤って良性 IP アドレスを分類した数が 1,537 個であった．Case4 で正しく悪性 IP アドレスであると分類できた数に着目すると，10,354 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 1,076 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，1,251 個であった．そのうち，誤って良性 IP アドレスを分類した数が 1,607 個であった．これらの結果から，IP アドレスクラス C のネットワークアドレス部のみを特徴ベクトルとして用いた Case3 で最高値を達成することができていない．また，関連研究[15]の精度が 85.1~88.5%であったのに対し，提案手法の精度は 81.2~81.7%であり，関連研究の精度を下回る結果が得られた．

IP アドレスクラス C において，悪性 IP アドレスと良性 IP アドレスの比率が 5:5 であるときの実験結果を示す．IP アドレスクラス C の悪性 IP アドレスと良性 IP アドレスの比率が 5:5 実験結果として，真陽性，偽陽性，真陰性，偽陰性を表 18 に示す．

表 18　IP アドレスクラス C の実験結果(5:5)

Table 18　The experimental result (5:5) of IP address of Class C

	真陽性	偽陰性	真陰性	偽陽性
Case1(k=8)	5,274	1,870	4,335	2,809
Case2(k=16)	5,274	1,870	4,335	2,809
Case3(k=24)	5,266	1,878	4,347	2,797
Case4(k=32)	4,933	2,211	4,502	2,642

IP アドレスクラス C の実験結果(5:5)を表 19 に示す．

表 19　IP アドレスクラス C の実験結果(5:5) (%)

Table 19　The experimental result (5:5) of IP address of Class C (%)

	精度	適合率	再現率
Case1(k=8)	67.25224	65.24805	73.82419
Case2(k=16)	67.25224	65.24805	73.82419
Case3(k=24)	67.28024	65.31068	73.71221
Case4(k=32)	66.03443	65.12211	69.05095

精度と適合率は, IP アドレスクラス C のネットワークアドレス部のみを特徴ベクトルとして用いた Case3 で最高値を示した．再現率は，Case1 と Case2 で最高値を示した．また，Case4 で，精度，適合率および再現率が最低値を示した．Case1 で正しく悪性 IP アドレスであると分類できた数に着目すると，5,274 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 1,870 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，4,335 個であった. そのうち, 誤って良性 IP アドレスを分類した数が 2,809 個であった．Case2 で正しく悪性 IP アドレスであると分類できた数に着目すると，5,274 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 1,870 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，4,335 個であった．そのうち，誤って良性 IP アドレスを分類した数が 2,809 個であった．Case3 で正しく悪性 IP アドレスであると分類できた数に着目すると，5,266 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 1,878 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，4,347 個であった．そのうち，誤って良性 IP アドレスを分類した数が 2,797 個であった．Case4 で正しく悪性 IP アドレスであると分類できた数に着目すると，4,933 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 2,211 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，4,502 個であった．そのうち，誤って良性 IP アドレスを分類した数が 2,642 個であった．したがって，悪性 IP アドレスと良性 IP アドレスの比率が 5:5 であるときのネットワークアドレス部を用いた判別は有効であると考えられる．また，Case4 で，精度，適合率および再現率が最低値を示したことから，ホストアドレス部まで用いた判別は適していないと言える．

4.4 評価実験 3：時間的変化を考慮した各 IP アドレスクラスを用いた判別

本節では，評価実験 3 の概要と実験結果について述べる．評価実験 3 では，各 IP アドレスを年度別に用いて判別を行う．評価実験 3 の目的は，ブラックリストの時間的な変化に応じて再学習を行った分類器の判別性能を確認することである．そのため，評価実験 3 では，最適な教師データの作成方法として，各 IP アドレスクラスの判別を年度別に行い，年度別に異なる特徴を生かすことができているかを評価する．評価は，各年度の精度で評価する．評価実験 3 に用いた IP アドレス数を，表 20，表 21，表 22 に示す．

表 20　評価実験 3 の IP アドレスクラス A の IP アドレス数

Table 20　The number of IP addresses of Class A used in evaluation experiment 3

	悪性 IP アドレス数	良性 IP アドレス数
2008 年	159,103	40,897
2009 年	22,537	40,897
2010 年	14,369	40,897
2011 年	9,538	40,897

表 21　評価実験 3 の IP アドレスクラス B の IP アドレス数

Table 21　The number of IP addresses of Class B used in evaluation experiment 3

	悪性 IP アドレス数	良性 IP アドレス数
2008 年	200	10,735
2009 年	22,537	10,735
2010 年	14,369	10,735
2011 年	945	10,735

表 22　評価実験 3 の IP アドレスクラス C の IP アドレス数

Table 22　The number of IP addresses of Class C used in evaluation experiment 3

	悪性 IP アドレス数	良性 IP アドレス数
2008 年	97,688	14,288
2009 年	11,619	14,288
2010 年	4,073	14,288
2011 年	1,854	14,288

4.4.1 実験結果

評価実験 1 の結果について述べる．実験結果は，Case1 を上位 8 ビット，Case2 を上位 16 ビット，Case 3 を上位 24 ビット，Case4 を上位 32 ビットと定義し，それぞれの場合について判別結果を評価した．まず，IP アドレスクラス A の実験結果として，2008 年の真陽性，偽陽性，真陰性，偽陰性を表 23 に示す．次に，2009 年の真陽性，偽陽性，真陰性，偽陰性を表 24 に示す．さらに，2010 年の真陽性，偽陽性，真陰性，偽陰性を表 25 に示す．最後に，2011 年の真陽性，偽陽性，真陰性，偽陰性を表 26 に示す．

表 23　IP アドレスクラス A の実験結果 (2008 年)

Table 23　The experimental result of IP address of Class A (2008 year)

	真陽性	偽陰性	真陰性	偽陽性
Case1(k=8)	118,876	40,227	29,246	11,651
Case2(k=16)	120,358	38,745	29,391	11,506
Case3(k=24)	120,285	38,818	29,419	11,478
Case4(k=32)	120,873	38,230	29,453	11,444

表 24　IP アドレスクラス A の実験結果 (2009 年)

Table 24　The experimental result of IP address of Class A (2009 year)

	真陽性	偽陰性	真陰性	偽陽性
Case1(k=8)	11,955	10,582	37,837	3,060
Case2(k=16)	11,955	10,582	37,579	3,318
Case3(k=24)	11,955	10,582	37,621	3,276
Case4(k=32)	11,955	10,582	37,612	3,285

表 25　IP アドレスクラス A の実験結果 (2010 年)

Table 25　The experimental result of IP address of Class A (2010 year)

	真陽性	偽陰性	真陰性	偽陽性
Case1(k=8)	7,529	6,840	37,982	2,915
Case2(k=16)	7,529	6,840	37,982	2,915
Case3(k=24)	7,529	6,840	37,982	2,915
Case4(k=32)	7,529	6,840	37,982	2,915

表 26　IP アドレスクラス A の実験結果 (2011 年)

Table 26　The experimental result of IP address of Class A (2011 year)

	真陽性	偽陰性	真陰性	偽陽性
Case1(k=8)	158	9,380	39,099	1,797
Case2(k=16)	491	9,047	38,579	2,317
Case3(k=24)	468	9,070	38,728	2,168
Case4(k=32)	405	9,133	38,697	2,199

図 17 に，IP アドレスクラスAの実験結果を示す.

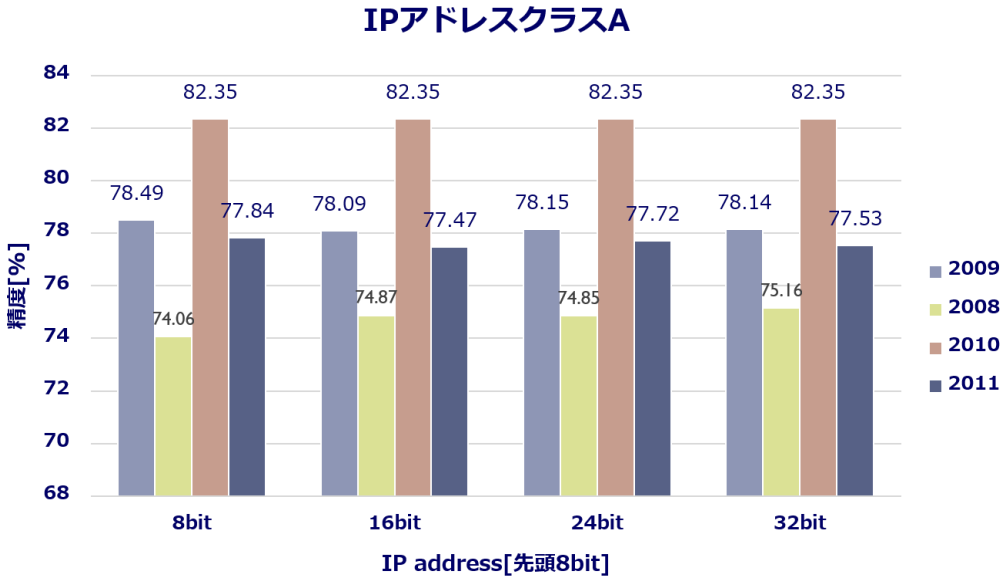


図 17　評価実験 3 の IP アドレスクラス A の判別精度

Figure 17　The result of evaluation experiment 3 in IP address of Class A

まず，2008 年の IP アドレスクラス A の結果について述べる．Case1 で正しく悪性 IP アドレスであると分類できた数に着目すると，118,876 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 40,227 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，29,246 個であった．そのうち，誤って良性 IP アドレスを分類した数が 11,651 個であった．Case2 で正しく悪性 IP アドレスであると分類できた数に着目すると，120,358 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 38,745 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，29,391 個であった．そのうち，誤って良性 IP アドレスを分類した数が 11,506 個であった．Case3 で正しく悪性 IP アドレスであると分類できた数に着目すると，120,285 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 38,818 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，29,419 個であった．そのうち，誤って良性 IP アドレスを分類した数が 11,478 個であった．Case4 で正しく悪性 IP アドレスであると分類できた数に着目すると，120,873 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 38,230 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，29,453 個であった．そのうち，誤って良性 IP アドレスを分類した数が 11,444 個であった．精度は，70%以上占める結果が得られた．

次に，2009 年の IP アドレスクラス A の結果について述べる．Case1 で正しく悪性 IP アドレスであると分類できた数に着目すると，11,955 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 10,582 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，37,837 個であった．そのうち，誤って良性 IP アドレスを分類した数が 3,060 個であった．Case2 で正しく悪性 IP アドレスであると分類できた数に着目すると，11,955 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 10,582 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，37,579 個であった．そのうち，誤って良性 IP アドレスを分類した数が 3,318 個であった．Case3 で正しく悪性 IP アドレスであると分類できた数に着目すると，11,955 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 10,582 個であった．また，正しく良性 IP アドレスであ

ると分類できた数に着目すると，37,621 個であった．そのうち，誤って良性 IP アドレスを分類した数が 3,276 個であった. Case4 で正しく悪性 IP アドレスであると分類できた数に着目すると, 11,955 個であった. そのうち, 誤って悪性 IP アドレスを分類した数が 10,582 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，37,612 個であった．そのうち，誤って良性 IP アドレスを分類した数が 3,285 個であった．精度は 70%以上を占める結果が得られた．また，IP アドレスクラス A のネットワークアドレス部である Case1 が Case2，Case3，Case4 より高精度を得られた．

さらに，2010 年の IP アドレスクラス A の結果について述べる．Case1 で正しく悪性 IP アドレスであると分類できた数に着目すると，7,529 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 6,840 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，37,982 個であった．そのうち，誤って良性 IP アドレスを分類した数が 2,915 個であった．Case2，Case3，Case4 も同様の結果が得られた．精度は 80%以上を占める結果が得られた．

最後に，2011 年の IP アドレスクラス A の結果について述べる．Case1 で正しく悪性 IP アドレスであると分類できた数に着目すると，158 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 9,380 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，39,099 個であった．そのうち，誤って良性 IP アドレスを分類した数が 1,797 個であった．Case2 で正しく悪性 IP アドレスであると分類できた数に着目すると，491 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 9,047 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，38,579 個であった．そのうち，誤って良性 IP アドレスを分類した数が 2,317 個であった．Case3 で正しく悪性 IP アドレスであると分類できた数に着目すると，468 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 9,070 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，38,728 個であった．そのうち，誤って良性 IP アドレスを分類した数が 2,168 個であった. Case4 で正しく悪性 IP アドレスであると分類できた数に着目すると，405 個であった. そのうち, 誤って悪性 IP アドレスを分類した数が 9,133 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，38,697 個であった．そのうち，誤って良性 IP アドレスを分類した数が 2,199 個であった．精度は 70%以上を占める結果が得られた．また，IP アドレスクラス A のネットワークアドレス部である Case1 が Case2，Case3，Case4 より高精度を得られた．

これらの結果から，精度は年度によってバラつきがみられた．また，2009 年と 2011 年は，IP アドレスクラス A のネットワークアドレス部である Case1 で Case2，Case3，Case4 より高精度を得られたため，ネットワークアドレス部を用いた判別は有効であると言える．また，教師データを年度別に分けることによって，得られる精度に差が出たことから，分類器を構成するために必要な情報として，経年変化に関する情報は適していると考えられる．

IP アドレスクラス B の実験結果を示す．まず, IP アドレスクラス B の実験結果として，2008 年の真陽性，偽陽性，真陰性，偽陰性を表 27 に示す．次に，2009 年の真陽性，偽陽性，真陰性，偽陰性を表 28 に示す．さらに，2010 年の真陽性，偽陽性，真陰性，偽陰性を表 29 に示す．最後に，2011 年の真陽性，偽陽性，真陰性，偽陰性を表 30 に示す．

表 27　IP アドレスクラス B の実験結果 (2008 年)

Table 27　The experimental result of IP address of Class B (2008 year)

	真陽性	偽陰性	真陰性	偽陽性
Case1(k=8)	1,407	513	10,389	346
Case2(k=16)	1,414	506	10,676	59
Case3(k=24)	1,414	506	10,676	59
Case4(k=32)	1,414	506	10,676	59

表 28　IP アドレスクラス B の実験結果 (2009 年)

Table 28　The experimental result of IP address of Class B (2009 year)

	真陽性	偽陰性	真陰性	偽陽性
Case1(k=8)	0	200	10,705	30
Case2(k=16)	145	55	10,709	26
Case3(k=24)	145	55	10,714	21
Case4(k=32)	145	55	10,715	20

表 29　IP アドレスクラス B の実験結果 (2010 年)

Table 29　The experimental result of IP address of Class B (2010 year)

	真陽性	偽陰性	真陰性	偽陽性
Case1(k=8)	0	185	10,375	360
Case2(k=16)	7	14,362	10,729	6
Case3(k=24)	7	14,362	10,729	6
Case4(k=32)	7	14,362	10,729	6

表 30　IP アドレスクラス B の実験結果 (2011 年)

Table 30　The experimental result of IP address of Class B (2011 year)

	真陽性	偽陰性	真陰性	偽陽性
Case1(k=8)	0	945	10,735	0
Case2(k=16)	0	945	10,723	12
Case3(k=24)	0	945	10,723	12
Case4(k=32)	0	945	10,723	12

図 18 に，IP アドレスクラス B の実験結果を示す.

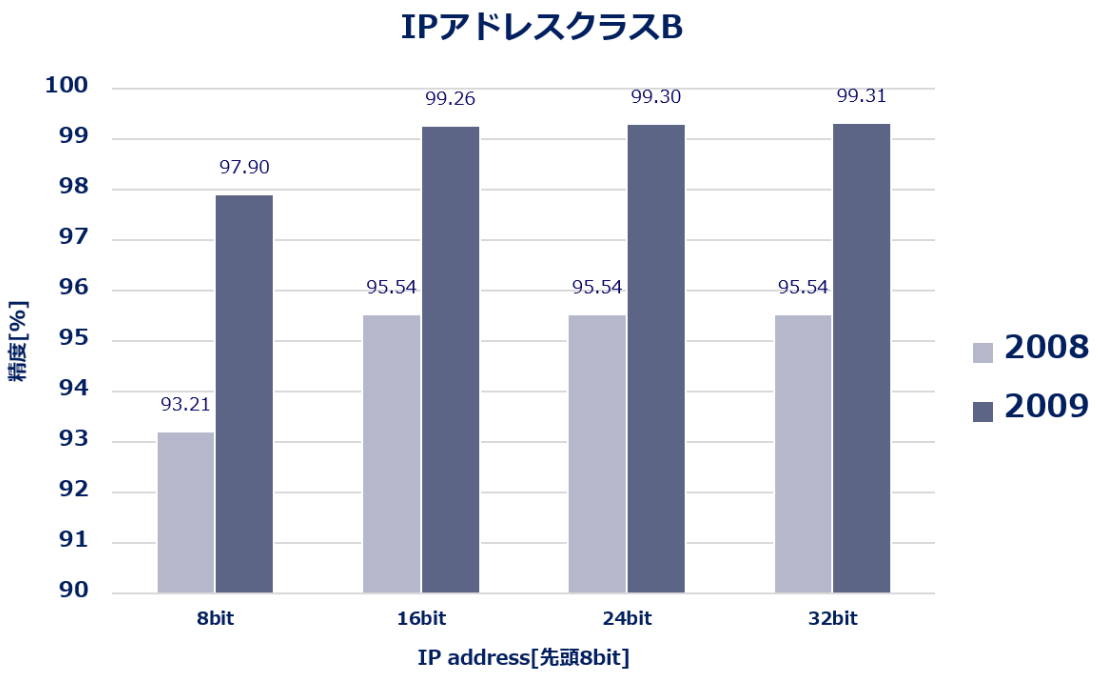


図 18　評価実験 3 の IP アドレスクラス B の判別精度

Figure 18　The result of evaluation experiment 3 in IP address of Class B

まず，2008 年の IP アドレスクラス B の結果について述べる．Case1 で正しく悪性 IP アドレスであると分類できた数に着目すると，1,407 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 513 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，10,389 個であった．そのうち，誤って良性 IP アドレスを分類した数が 346 個であった．Case2 で正しく悪性 IP アドレスであると分類できた数に着目すると，1,414 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 506 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，10,676 個であった．そのうち，誤って良性 IP アドレスを分類した数が 59 個であった．Case3 で正しく悪性 IP アドレスであると分類できた数に着目すると，1,414 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 506 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，10,676 個であった．そのうち，誤って良性 IP アドレスを分類した数が 59 個であった．Case4 で正しく悪性 IP アドレスであると分類できた数に着目すると，1,414 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 506 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，10,676 個であった．そのうち，誤って良性 IP アドレスを分類した数が 59 個であった．判別精度を見ると，関連研究[15]の精度が 84.6~86.2%に対し，判別精度が 90%以上を占めた．

次に，2009 年の IP アドレスクラス B の結果について述べる．Case1 で正しく悪性 IP アドレスであると分類できた数に着目すると，0 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 200 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，10,705 個であった．そのうち，誤って良性 IP アドレスを分類した数が 30 個であった．Case2 で正しく悪性 IP アドレスであると分類できた数に着目すると，145 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 55 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，10,709 個であった．そのうち，誤って良性 IP アドレスを分類した数が 26 個であった．Case3 で正しく悪性 IP アドレスである

と分類できた数に着目すると，145 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 55 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，10,714 個であった．そのうち，誤って良性 IP アドレスを分類した数が 21 個であった. Case4 で正しく悪性 IP アドレスであると分類できた数に着目すると, 145 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 55 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，10714 個であった．そのうち，誤って良性 IP アドレスを分類した数が 20 個であった．判別精度を見ると，関連研究[15]の精度が 84.6~86.2%に対し，判別精度が 90%以上を占めた．2010 年以降の判別は，IP アドレス数が極端に少なく判別が困難な状況であったため，悪性 IP アドレスの判別ができなかった．

IP アドレスクラス C における実験結果を示す．まず，IP アドレスクラス C の実験結果として，2008 年の真陽性，偽陽性，真陰性，偽陰性を表 31 に示す．次に，2009 年の真陽性，偽陽性，真陰性，偽陰性を表 32 に示す．さらに，2010 年の真陽性，偽陽性，真陰性，偽陰性を表 33 に示す．最後に，2011 年の真陽性，偽陽性，真陰性，偽陰性を表 34 に示す.

表 31　IP アドレスクラス C の実験結果 (2008 年)

Table 31　The experimental result of IP address of Class C (2008 year)

	真陽性	偽陰性	真陰性	偽陽性
Case1(k=8)	86,225	11,463	9,456	4,832
Case2(k=16)	86,225	11,463	9,456	4,832
Case3(k=24)	86,225	11,463	9,456	4,832
Case4(k=32)	86,225	11,463	9,456	4,832

表 32　IP アドレスクラス C の実験結果 (2009 年)

Table 32　The experimental result of IP address of Class C (2009 year)

	真陽性	偽陰性	真陰性	偽陽性
Case1(k=8)	6,292	5,327	12,544	1,744
Case2(k=16)	6,756	4,863	12,765	1,523
Case3(k=24)	6,774	4,845	12,762	1,526
Case4(k=32)	7,124	4,495	12,756	1,532

表 33　IP アドレスクラス C の実験結果 (2010 年)

Table 33　The experimental result of IP address of Class C (2010 year)

	真陽性	偽陰性	真陰性	偽陽性
Case1(k=8)	1,156	2,917	13,119	1,169
Case2(k=16)	1,156	2,917	13,119	1,169
Case3(k=24)	1,156	2,917	13,119	1,169
Case4(k=32)	912	3,161	13,237	1,051

表 34　IP アドレスクラス C の実験結果 (2011 年)

Table 34　The experimental result of IP address of Class C (2011 year)

	真陽性	偽陰性	真陰性	偽陽性
Case1(k=8)	0	1,854	14,288	0
Case2(k=16)	0	1,854	14,288	0
Case3(k=24)	0	1,854	14,288	0
Case4(k=32)	0	1,854	14,288	0

図 19 に，IP アドレスクラス C の実験結果を示す.

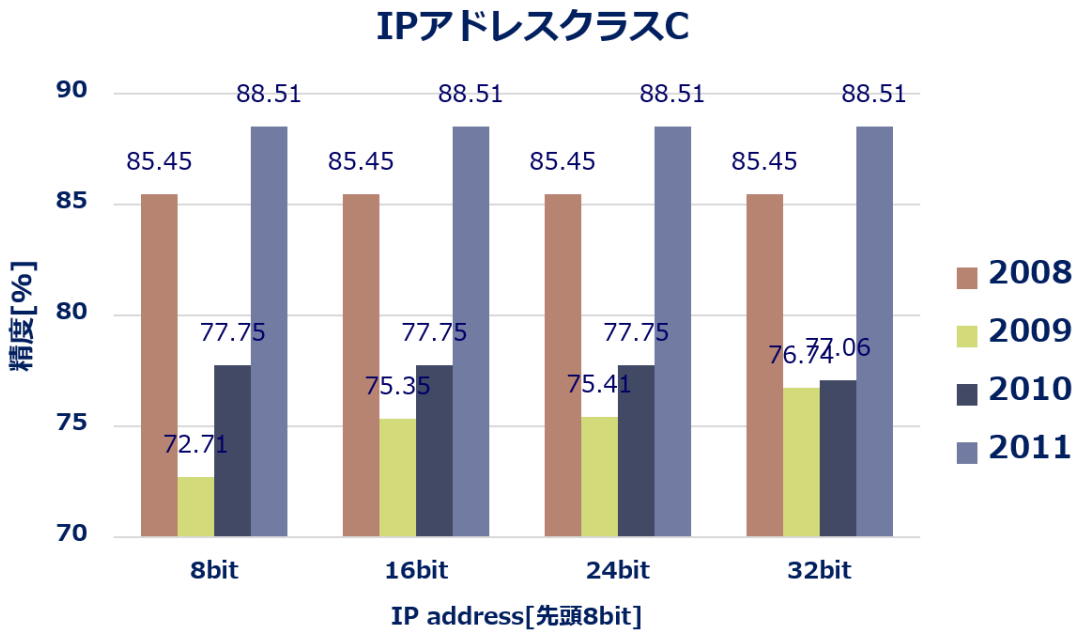


図 19　評価実験 3 の IP アドレスクラス C の判別精度

Figure 19　The result of evaluation experiment 3 in IP address of Class C

まず，2008 年の IP アドレスクラス C の結果について述べる．Case1 で正しく悪性 IP アドレスであると分類できた数に着目すると，86,225 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 11,463 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，9,456 個であった．そのうち，誤って良性 IP アドレスを分類した数が 4,832 個であった．Case2，Case3，Case4 も同様の結果が得られた．精度は 85%以上を占める結果が得られた．

次に，2009 年の IP アドレスクラス C の結果について述べる．Case1 で正しく悪性 IP アドレスであると分類できた数に着目すると，6,292 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 5,327 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，12,544 個であった．そのうち，誤って良性 IP アドレスを分類した数が 1,744 個であった．Case2 で正しく悪性 IP アドレスであると分類できた数に着目すると，6,756 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 4,863 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，12,765 個であった．そのうち，誤って良性 IP アドレスを分類した数が 1,523 個であった．Case3 で正しく悪性 IP アドレスであると分類できた数に着目すると，6,774 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 4,845 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，12,762 個であっ

た．そのうち，誤って良性 IP アドレスを分類した数が 1,526 個であった．Case4 で正しく悪性 IP アドレスであると分類できた数に着目すると，7,124 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 4,495 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，12,756 個であった．そのうち，誤って良性 IP アドレスを分類した数が 1,532 個であった．精度は 70%以上を占める結果が得られた．

さらに，2010 年の IP アドレスクラス C の結果について述べる．Case1 で正しく悪性 IP アドレスであると分類できた数に着目すると，1,156 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 2,917 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，13,119 個であった．そのうち，誤って良性 IP アドレスを分類した数が 1,169 個であった．Case2，Case3 も同様の結果が得られた．Case4 で正しく悪性 IP アドレスであると分類できた数に着目すると，912 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 3,161 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，13,237 個であった．そのうち，誤って良性 IP アドレスを分類した数が 1,051 個であった．精度は 70%以上を占める結果が得られた．

最後に，2011 年の IP アドレスクラス C の結果について述べる．Case1 で正しく悪性 IP アドレスであると分類できた数に着目すると，0 個であった．そのうち，誤って悪性 IP アドレスを分類した数が 1,854 個であった．また，正しく良性 IP アドレスであると分類できた数に着目すると，14,288 個であった．そのうち，誤って良性 IP アドレスを分類した数が 0 個であった．Case2，Case3，Case4 も同様の結果が得られた．精度は 80%以上を占める結果が得られた．関連研究[15]の精度が 85.1~88.5%であったのに対し，2008 年と 2011 年の判別精度が 85%割まで向上したことが確認できた．

4.5 考察

本節では，評価実験 1~3 の結果について考察する．まず，評価実験 1 について述べる．次に，評価実験 1 について述べる．最後に，評価実験 3 のついて述べる．

まず，評価実験 1 の実験結果について述べる．実験結果より，精度が低い値を示したことから，ブラックリストを用いた不正 Web サイトの検出は，汎化能力が低く，未知の Web サイトに対応できる能力を持たないことが挙げられる．

次に，評価実験 2 について述べる．実験結果より，IP アドレスクラス A は，ネットワークアドレス部のみの判別で十分な精度を保つことができるため，提案手法は未知の不正 Web サイトに対して有効であるといえる．一方，IP アドレスクラス B と IP アドレスクラス C では，IP アドレスクラス A と比較して，全体的に精度が低い結果となった．考えられる要因として，2 つ挙げられる．まず，教師データセットの IP アドレス数が極端に少ないため，特徴がはっきり表れていない可能性がある点が挙げられる．次に，悪性 IP アドレスの特徴に経年変化が起きている可能性がある点が挙げられる．したがって，ブラックリスト全体を用い，時間的な変化を想定しない分類器の場合は，IP アドレスクラス A の判別は高精度であったが，IP アドレスクラス B と IP アドレスクラス C の判別精度は芳しくない結果となった．

最後に，評価実験 3 の実験結果について述べる．3.6 節より，悪性 IP アドレスの特徴に経年変化がみられることが判明した．これらの情報を踏まえて，悪性 IP アドレスの特徴の経年変化を考慮した判別を行うことにより，判別精度を向上させることができた．また，関連研究[15]では，IP アドレスの全 bit を特徴として分類器を構成していたが，提案手法である IP アドレスのネットワーク部分のみを用いて次元数を抑えた分類器でも，既知の不正 Web サイトの IP アドレスを蓄積したブラックリストにおける出現 IP アドレス分布の時間的な変化を取り入れる

ことで，関連研究と同等の精度を得ることができた．

これらの結果から，悪性 IP アドレスデータ群（ブラックリスト）をそのまま蓄積して使用する方法では，精度を保つことが困難であったが，IP アドレスクラスごとに教師データの状態を変えることで，年度別に異なる特徴を維持することができ，判別精度が保たれたと考えられる．したがって，IP アドレスクラスの中でも，変動のあるネットワークアドレス群の範囲を見つけることで，未知の Web サイトに対応していくことが可能であると考えられる．

第5章　結言

5.1　まとめ

本稿は，IP アドレスを用いて，未知の Web サイトを検出し，正規と不正に判別する手法を提案した．また，未知の不正 Web サイトの判別には，IP アドレスのネットワークアドレス部のみを用いることで，判別に必要なコストを軽減しながら，正規 Web サイトと不正 Web サイトに判別する手法を提案した．ブラックリストに登録されている IP アドレスを元に特徴を抽出し，未知の Web サイトを判別するが，ブラックリストの悪性 IP アドレスの特徴に経年変化が生じることが分析した結果より確認された．これが分類精度に与える影響を検討するために，(ブラックリストそのもの，ブラックリストの変化による再学習なし，ブラックリストの変化による再学習あり)を構成して精度を比較する実験を行った．ブラックリストを用いた不正 Web サイトの検出は，精度が低い値を示したことから，汎化能力が低く，未知の Web サイトに対応できる能力を持たないことが挙げられる．ブラックリストの変化による再学習なしの実験では，IP アドレスクラス A では，高精度な判別ができ，提案した判別手法の有効性を確認できた．一方で，IP アドレスクラス B および IP アドレスクラス C における判別精度はそれほど高くなかった．ブラックリストの変化による再学習ありの実験では，悪性 IP アドレスの特徴の経年変化を考慮した判別を行うことにより，判別精度を向上させることができた．また，関連研究[15]では，IP アドレスの全 bit を特徴として分類器を構成していたが，本研究では IP アドレスのネットワーク部分のみを用いた分類器でも，既知の不正 Web サイトの IP アドレスを蓄積したブラックリストにおける出現 IP アドレス分布の時間的な変化を取り入れることで関連研究と同等の精度を得ることを示した．これらの結果から，悪性 IP アドレスデータ群（ブラックリスト）をそのまま蓄積して使用する方法では，精度を保つことが困難であったが，IP アドレスクラスごとに教師データの状態を変えることで，年度別に異なる特徴を維持することができ，判別精度が保たれたと考えられる．

今後は，より有効な判別を行うために，各 IP アドレスクラスにおけるデータの更なる分析を行い，より効果的な教師データの生成手法の検討を行う必要がある．検討事項である一つに，CIDR を取り入れた判別手法を考慮する必要がある．CIDR による IP アドレス配布状況を考慮に入れることにより，さらなる判別精度向上の可能性はあるが，文献[20]による調査結果では，IP アドレスクラス C 相当の 24bits prefix によるアドレス使用が多いため，それ以外の prefix 長でアドレスを利用している場合の判別精度への影響が不明であり，更に具体的な調査・検討が必要となる．さらに，IP アドレスクラスごとにデータ数に差がある場合でも判別精度を保つ方法を検討する．最後に，IP アドレスを用いた判別手法において，一度悪性と判別された IP アドレスが破棄され，新たにそのアドレスに正規 Web サイトが構築された場合に，どのような手続きで良性 IP アドレスとみなすように判別を変更するかを考慮する必要がある．以上の項目を検討した上で，提案システムの精度向上が達成されるかどうかを確認する必要がある．

5.2　今後の展望

今後の展望として，特に判別精度が安定しない結果となった IP アドレスクラス B と IP アドレスクラス C の改善を行う必要がある．まず，IP アドレスクラス B は極端に IP アドレス数が少ないため，教師データが少ない状態でも判別精度を保つ方法を検討する．次に，IP アドレス

クラス C の更なる特徴分析を行う．単純な年度比較ではなく，IP アドレスの配布ポリシーの変化があったタイミングなどでさらに細かく区切り，IP アドレスクラス C に適する判別方法を検討する．最後に，悪性 IP アドレスと良性 IP アドレスの特徴を最新に保つ手法の検討することにより，将来的には，データを全て差し替えることなく，限られた範囲のデータのみ更新できるようになると考えている．

謝辞

本研究を進めるにあたり，本学中村嘉隆准教授，高橋修教授には，お忙しい中にも関わらず，研究に関する助言をはじめ，熱心にご指導していただきました．ここに深く感謝申し上げます．本論文の審査を担当していただいた，稲村浩教授，白石陽教授には副査を快く引き受けてくださるだけでなく，学内の研究発表に対する建設的なコメントやアドバイスを多くいただきました．重ねてお礼を申し上げます．また，本研究を進めるにあたりデータをご提供くださったMWS にお礼を申し上げます．最後になりますが，私を支えて頂きました中村嘉隆准教授，稲村浩教授，中村研究室，稲村研究室の皆様にも重ねてお礼を申し上げます．

参考文献

[1] 警察庁広報資料，平成 25 年中のインターネットバンキングに係る不正送金事犯の発生状況等について, <https://www.npa.go.jp/cyber/pdf/H270212_banking.pdf> [参照 2017-1-17].

[2] 警察庁広報資料: 平成 26 年中のインターネットバンキングに係る不正送金事犯の発生状況等について<https://www.npa.go.jp/cyber/pdf/H270212_banking.pdf> [参照 2017-1-17].

[3] 独立行政法人情報処理推進機構:2016 年版 情報セキュリティ 10 大脅威, <https://www.ipa.go.jp/files/000051691.pdf> [参照 2017-5-31].

[4] 独立行政法人情報処理推進機構:2017 年版 情報セキュリティ 10 大脅威, <https://www.ipa.go.jp/files/000058504.pdf> [参照 2017-5-31].

[5] トレンドマイクロ: Web レピュテーション, <http://www.trendmicro.co.jp/why-trendmicro/spn/features/web/index.html> [参照 2016-8-11].

[6] M. A. Rajab, L. Ballard, N. Jagpal, P. Mavrommatis, D. Nojiri, N. Provos, and L. Schmidt,"Trends in circumventing web-malware detection, Google Technical Report, 2011.

[7] R. Farmer, and B. Glass, "Building Web Reputation Systems, " Yahoo! Press, 2010.

[8] What is IDS/IPS? | JUNIPER NETWORKS, <https://www.juniper.net/us/en/products-services/what-is/ids-ips/> [Accessed Oct 19, 2017]

[9] シスコシステムズ: 侵入防御システム（IPS：Intrusion Prevention System） <https://www.cisco.com/c/ja_jp/about/technology-commentary/tech-2006/intrusion-prevention-system-ips-intrusion-prevention-system.html> [参照 2017-8-27].

[10] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, :Beyond blacklists: learning to detect malicious web sites from suspicious urls, Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining (KDD'09), pp. 1245–1254, 2009.

[11] 劉亦晨: DNS 情報による悪意のあるサイトの検出法, 2012 年度 早稲田大学大学院 基幹理工学研究科 情報理工学専攻 修士論文，2012.

[12] 日立ソリューションズ: 情報セキュリティブログ， <http://securityblog.jp/words/2898.html> [参照 2017-1-17].

[13] L. Bilge, E. Kirda, C. Kruegel, and M. Balduzzi,:Exposure Finding Malicious Domains Using Passive DNS Analysis, Proceedings of the 18th Annual Network & Distributed System Security Symposium (NDSS Symposium 2011), 2011.

[14] 田中晃太郎, 長尾篤, 森井昌克: DNS ログからの不正 Web サイト抽出について－解析手法とその匿名化－, コンピュータセキュリティシンポジウム 2013 論文集, Vol.2013, No.4, pp.132-138 (2013).

[15] D. Chiba, K. Tobe, T. Mori, and S. Goto, :Detecting Malicious Websites by Learning IP Address Features, Proceedings of the IEEE/IPSJ 12th International Symposium on Applications and the Internet(SAINT2012), pp.29-39, 2012.

[16] 千葉大紀，森達哉，後藤滋樹: 悪性 Web サイト探索のための優先巡回順序の選定法, コンピュータセキュリティシンポジウム 2012 論文集，Vol.2012，No.3，pp.805-812 (2012).

[17] アンドリュー・S・タネンバウム,デイビッド・J・ウエザロール:コンピュータネットワーク第 5 版,日経 BP 社, 2013

[18] 高田雄太，寺田真敏，村上純一，笠間貴弘，吉岡克成，畑田光弘: マルウェア対策のための研究用データセット～MWS Datasets 2016～, 情報処理学会研究報告, Vol.2016-CSEC-74, No.17, pp. 1-8, 2016.

[19] Alexa Internet, Inc.: The top 500 sites on the web," <http://www.alexa.com/topsites> [参照 2017-8-27].

[20] University of Oregon Route Views Project, <http://www.routeviews.org/> [Accessed December 27, 2017]

発表・採録実績

発表

[I] 金澤しほり，中村嘉隆，稲村浩，高橋修，"IP アドレスクラスにおけるネットワークアドレスの特徴を用いた未知の不正 Web サイト判別手法，"情報処理学会マルチメディア, 分散, 協調とモバイルシンポジウム(DICOMO2016)論文集, Vol.2016, pp.806-812, 2016. 「査読付き」

[II] 金澤しほり，中村嘉隆，稲村浩, 高橋修，"未知の不正 Web サイト判別のための IP アドレスクラスの特徴分析，"コンピュータセキュリティシンポジウム 2016 (CSS2016) 論文集，Vol.2016，No.2，pp.777-783，2016 年 10 月.

[III] Shihori Kanazawa, Yoshitaka Nakamura, Hiroshi Inamura, and Osamu Takahashi, "A classifying method of unknown malicious websites using address features of each network address class," Proceedings of the International Workshop on Informatics (IWIN2017), pp.261-267, September 2017. 「査読付き」

[IV] 金澤しほり，中村嘉隆，稲村浩，高橋修，"悪性 IP アドレスの分布特徴に基づく未知の Web サイトの判別手法，"コンピュータセキュリティシンポジウム 2017 (CSS2017) 論文集，Vol.2017，pp.1076-1084，2017 年 10 月.

[V] Shihori Kanazawa, Yoshitaka Nakamura, Hiroshi Inamura, and Osamu Takahashi, "Classification of unknown Web sites based on yearly changes of distribution information of malicious IP addresses," Proceedings of the 9th IFIP International Conference on New Technologies, Mobility & Security (NTMS2018), February 2018. (to appear) 「査読付き」

[VI] Shihori Kanazawa, Yoshitaka Nakamura, Hiroshi Inamura, and Osamu Takahashi, "Classification method of unknown web sites based on distribution information of malicious IP addresses," International Journal of Informatics Society (IJIS), Vol.10, No.1, June 2018. 「採録決定」

図目次

表目次